eConsumer Emerging Technologies

LCMS Access Control User Guide

Business Client	:	**Sun Microsystems, Inc.**
Project Name	:	**Sun JavaBadge**
Prepared by	:	Jennifer Ilk
Last Updated Date	:	11/13/01
Document Version	:	V 1.4
Document #	:	
Soft Copy Name	:	
Document Classification	:	**CITIGROUP CONFIDENTIAL**

citi

Change History

Date of Update	Document Version	Update Description/ High-Level Change	Author
9/4/01	1.0	First Review Draft	J. Ilk
9/5/01	1.1	Updates from first review comments from J. Pan, H. Garcia, G. Han, ... ▪ Added Test Environment LCMS Admin Card Issuance instructions (Appendix D) ▪ Added information about certificate re-issuance notification in Account Request File Requirements (3.3.3) ▪ Added Target Audience ▪ Added port 8144 and 80 explanation to Section 2.2 ▪ Added a process summary after each issuing use case in Sections 3, 4, 5 ▪ Added an overview section to Certificate Re-issuance (6.1)	J. Ilk
9/17/01	1.2	▪ Updated Certificate re-issuance section	J. Ilk
9/26/01	1.3	▪ Determined that Gold 1.2 c2 will be used for Admin Card Issuing/Initialization (until Gold 2.0 SP1 product is released	J. Ilk
10/26/01	1.4	▪ Updated Appendix D ▪ Updated 1-way SSL port to be 7001 instead of 7002 ▪ Added notes to section 4.3 and 4.4	J. Ilk

citi

Table of Contents

1. Introduction

This document is a user guide for issuing LCMS Administrator Cards, User IDs/passwords and system user certificates to access the Arterium application. It describes how to perform the steps for each of the roles involved in establishing access control for the LCMS system.

1.1 Target Audience

This document is intended for anyone within Citibank who has a role in the LCMS Access Control Process for the Sun Java™Badge project. There are instructions for each role in the end-to-end process. These roles include:

- Program Administrator
- Program Fulfillment
- Business Manager
- Arterium Security Administrator
- LDAP Operator
- RA Administrator
- System User Administrator
- LCMS Admin Card Initializer
- Issuing Workstation Operator

A separate document for Sun Microsystems employees explains the roles they play.

1.2 Document Replacement

This document combines and updates the information that used to be provided in the following documents:

1.3 Additional references

1.4 Utilities required

The following software utilities are required in order to execute the various steps described in this document:

- PIN Generation Utility (Netscape CMS)
- LDIF Utility (ET created)
- CDL Utility (ET created)
- CertCheck.pl (ET created)
- PGP
- Perl

1.5 Open Issues

- Need to write and document the CertCheck.pl script
- Update Admin Card Issuing and Initialization workstation software to Gold 2.0 SP1 when it is available for general release

2 Access Control Overview

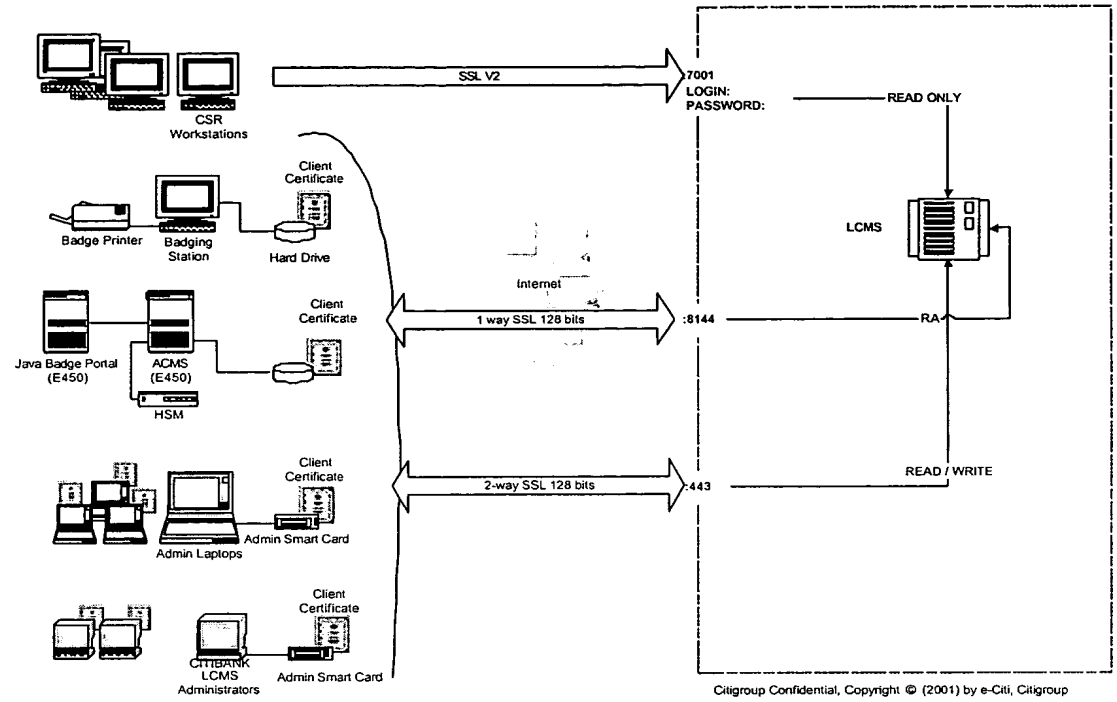
2.1 Overview

There are two ways to access the LCMS. One is with a User ID and password via a one-way SSL connection. The other is with a client based PKI certificate via a two-way SSL connection. The one-way SSL connection is for those users with read only access to the LCMS. Examples of these types of users are Customer Help Desk or Customer Service Representative employees. The two-way SSL connection is for users or systems that have write access to the LCMS. Examples of these types of users are customer Security officers or badging systems. Individual user client certificates are stored on an LCMS Administrator Smart card issued by Citibank. "System user" client certificates are stored on the system's hard drive or HSM, depending on what the system will support.

In order to be granted access to the LCMS, the user's Program Administrator must submit an access request to the Citibank LCMS Business Manager for review and approval. Once the request is approved, it is passed to the Arterium Security Administrator and other LCMS system operators for processing.

2.2 System Architecture

CSRs or Help Desk Representatives within Sun establish a one-way SSL connection to the LCMS through port 7001. Those with client certificates establish a two-way SSL connection to the LCMS through port 443. There is also access to the Citibank LCMS Registration Authority via port 8144 to request and retrieve new client certificates. No access is allowed through the standard HTTP port 80. This process is explained further throughout this document. The following diagram shows the different types of access to the LCMS:



This architecture assumes the Netscape CMS and iPlanet Directory Server will be utilized to provide the certificate based access control to the LCMS. If another CMS or LDAP platform will be used, the specific processes may have to be modified.

2.2.1 Access Control with User ID/Password

2.2.1.1 Guest clients

Access thru known port **80** (http) is not allowed.

2.2.1.2 Clients accessing with a password

Clients accessing the LCMS with read only privilege are required to be issued a "User ID/ password" access.

Protocol

The protocol is one-way SSL and does not require client authentication.

URL

The connection is established with the LCMS on a specific URL and the port number **7001**

https://cardmanagement.citibank.com:7002/arterium

ROLES WITH THIS ACCESS

- hostingAdminOfficer – LCMS Hosting administrators who require access to upload files to the LCMS
- sunHelpDeskOfficer – Sun Resolution Center users, or others who require read-only access to the system

citi

2.2.2 Access Control with a Certificate

2.2.2.1 Certificate request for System Users

Clients accessing LCMS for certificate issuance and download have access via https using port **8144**.

Protocol

The protocol is one-way SSL so it does not requires client authentication. The process for certificate issuance ensures that certificates are issued only to trusted entities.

URL

The connection is established with the LCMS on a specific URL and the port number **8144**

https://cardmanagement.citibank.com8144/arterium

2.2.2.2 Clients accessing with a certificate

Clients accessing LCMS with read/write privilege on the database must have a certificate issued by the LCMS's Certificate Authority.

Protocol

The protocol is two-way SSL so it requires client authentication.

URL

The connection is established with the LCMS on a specific URL and the port number **443**

https://cardmanagement.citibank.com/arterium

ROLES WITH THIS ACCESS

- citiAdminOfficer – Citibank users who require write access to the LCMS System.
- sunAdminOfficer – Sun Badging Officers
- Vendor – Vendors who require access to upload files to the LCMS
- activCardServer – System user account for Sun JavaBadge Portal or ACMS. This server requires read/write XML access to the LCMS
- badgingStation – System user account for the Sun Badging station. This system requires read/write XML access to the LCMS

2.3 Roles and Responsibilities

The following gives a brief overview of the roles and responsibilities involved with requesting, granting and using access to the LCMS. Each of these roles and responsibilities is described in greater detail throughout this document.

2.3.1 Overview

There are many roles in the LCMS Access Request Process. These roles are dispersed across the Citibank organization, and at times multiple organizations will require the same role. The following is a list of the LCMS Access Request process roles by the Citibank organization that fills each role. A more detailed description of the role in each of the access request process scenarios follows this overview.

LCMS Hosting, Citibank Vendor (i.e. Schlumberger), and Arterium Program Administration (i.e. eConsumer Emerging Technologies, eBusiness eSolutions)

- Program Administrator
- Program Fulfillment
- New LCMS Admin
- New UID/Password User

citi

eBusiness eSolutions:
- Business Manager

LCMS Hosting:
- Arterium Security Administrator
- LDAP Operator
- RA Administrator
- Issuing Workstation Operator

eConsumer Emerging Technologies:
- LCMS Admin Card Initializer

The only role that most likely will not be performed by a Citibank organization is the New System User Admin, which is part of the System User Certificate Issuing process. This role is for remote servers that need to connect to Arterium via XML messaging. Sun Microsystems will have users who play this role.

2.3.2 LCMS Administration Card Issuing Role Summary

LCMS Admin Card issuing roles fall into four groups that either issue the cards or rely on them.

Card Initialization
- LCMS Admin Card Initializer: A one-time preparatory role. Cards are initialized and card data is captured. Cards and data are sent to the Issuing Workstation Operator

Relying Organization(s)

The Program Administrator and Fulfillment roles are specified separately to increase the security of the overall process. However, it is up to the Relying Organization to decide whether these roles are staffed separately or not. There may be multiple Relying Organizations, including, but not limited to, Citibank, Citibank customers, and vendors to Citibank.

- Program Administrator: Overall administrator of LCMS admin cards and administrators for a relying organization. Issues request for new admin cards, and receives confirming notification of issued cards and card data.
- Program Fulfillment: Fulfillment officer at relying organization. Receives cards and distributes appropriately. Separation of duties from Program Administrator provides increased security for cards and sensitive data.
- New LCMS Admin: New user of LCMS admin card. Roles and responsibilities are not covered in this document. Please see appropriate documentation issued by the relying organization.

Business Management
- Business Manager. Role with ultimate responsibility for and approval of requests for new LCMS Administrator Cards.

Card Personalization

The following roles are assumed to be located at the same site and that internal security mechanisms will be used appropriately in the internal transmission and delivery of data and cards.

- Arterium Security Administrator: Administrator of the card issuing process preformed at the issuing site. Receives and logs requests for new admin cards, confirms proper number of cards were initialized and certificates were generated, and sends notification / card data to admin card requestor. May generate reports or other MIS to support Business Management of LCMS administration and access.
- LDAP Operator: Processes and updates new admin card data file and creates special web accounts for processing pre-authorized certificate requests.
- Issuing Workstation Operator: Inventories cards. Accesses web accounts, generating keys and downloading certificates to the cards. Updates admin card data file. Separation of roles from LDAP Operator provides increased security for card personalization.

citi

2.3.3 UID/Password Issuing Role Summary

User ID/Password issuing roles fall into three groups that either issue the UID/passwords or rely on them.

Relying Organization(s)
There may be multiple Relying Organizations, including, but not limited to, Citibank, Citibank customers, and vendors to Citibank.

- Program Administrator: Overall administrator of UID/passwords and users for a relying organization. Issues request for new UID/password accounts, and receives confirming information with UID/password data.
- New UID/password User: New user of LCMS UID/password. Roles and responsibilities are not covered in this document. Please see appropriate documentation issued by the relying organization.

Business Management
- Business Manager. Role with ultimate responsibility for and approval of requests for new LCMS UID/passwords.

UID/Password Creation
The following roles are assumed to be located at the same site and that internal security mechanisms will be used appropriately in the internal transmission and delivery of account data

- Arterium Security Administrator: Administrator of UID/password issuing process performed at issuing site. Receives and logs requests for new accounts, confirms proper number of accounts were generated, and sends notification / account data to account requestor. May generate reports or other MIS to support Business Management of LCMS administration and access.
- LDAP Operator: Processes and updates account data file.

2.3.4 System User Certificate Issuing Role Summary

System user certificate issuing roles fall into three groups that either issue certificates or rely on them.

Relying Organization(s)
There may be multiple Relying Organizations, including, but not limited to, Citibank, Citibank customers, and vendors to Citibank.

- Program Administrator: Overall administrator of LCMS system user certificates and for a relying organization. Issues request for new system user certificates, and receives confirming notification of issued certificates.
- New System User Admin: New user of LCMS system user certificates. Roles and responsibilities are not covered in this document. Please see appropriate documentation issued by the relying organization.

Business Management
- Business Manager. Role with ultimate responsibility for and approval of requests for new LCMS System user certificates.

System User Certificate Generation
The following roles are assumed to be located at the same site and that internal security mechanisms will be used appropriately in the internal transmission and delivery of certificate data.

- Arterium Security Administrator: Administrator of system user certificate issuing process performed at issuing site. Receives and logs requests for new system user certificates, confirms proper number system accounts were generated, and sends notification of activated accounts to system user account requestor. May generate reports or other MIS to support Business Management of LCMS administration and access.
- LDAP Operator: Processes and updates system user account data file, creates special web accounts for processing pre-authorized certificate requests.

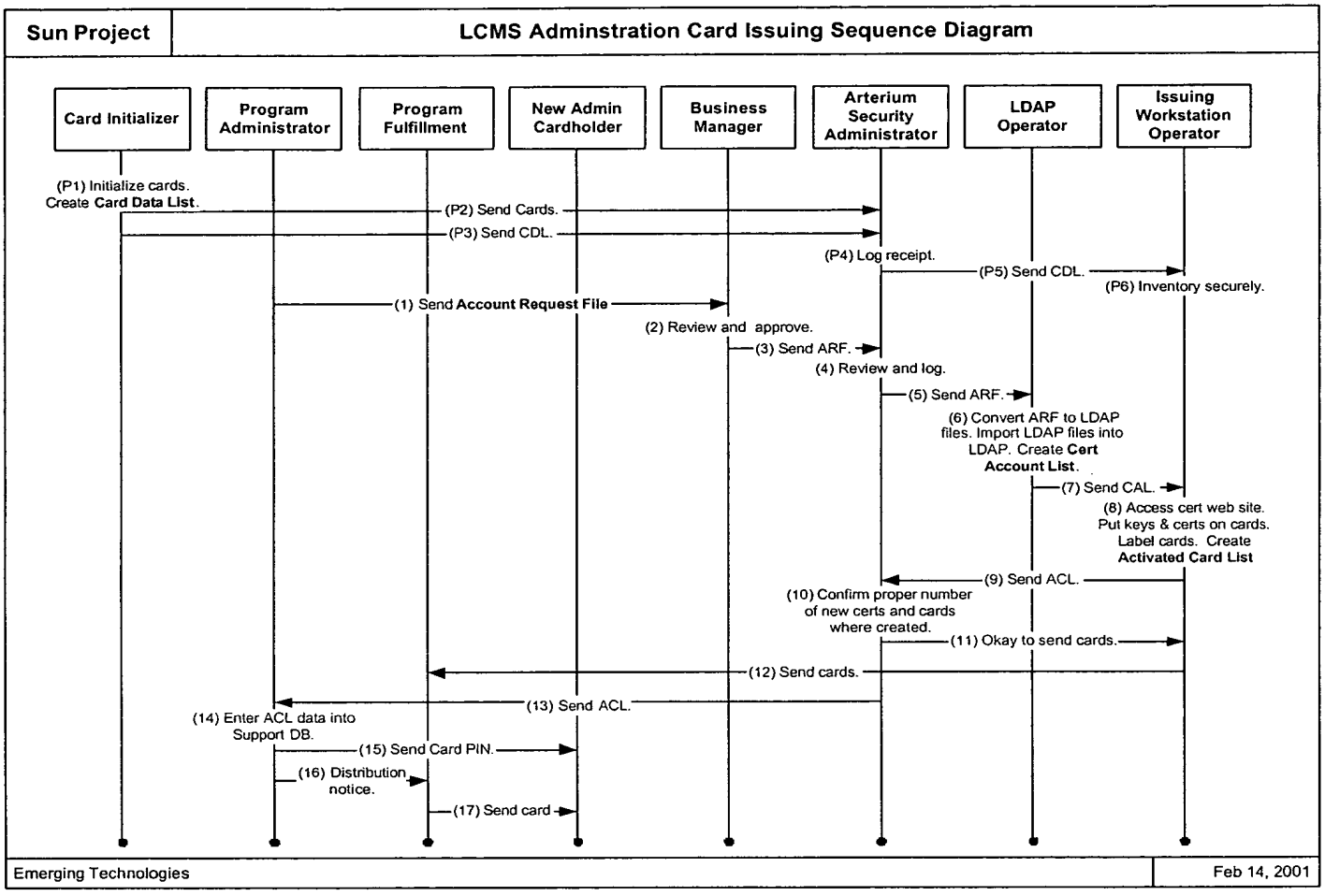
citi

- Registration Authority (RA) Administrator: Approves new certificate requests for CMS by comparing request to approved system account list. This role may be played by the Arterium Security Administrator.

citi

3 LCMS Administration Card Issuing Process

The following diagram shows the overall process for LCMS Administration Card Issuance.



Each of the steps and the utilities and programs required to complete the steps are described in the following pages. Here is a summary of the steps and the sections in which they are described:

1. LCMS Administrator Card Initialization (Steps P1-P3) – Section 3.1
2. LCMS Administrator Card Receipt and Storage (Steps P4-P6) – Section 3.2
3. Account Request and Approval (Steps 1-3) – Section 3.3
4. Account Request File Processing (Steps 4-7) – Section 3.4
5. LCMS Administrator Card Personalization (Steps 8-9) – Section 3.5
6. LCMS Administrator Card Confirmation and Delivery (Steps 10-13) – Section 3.6
7. LCMS Administrator Card Fulfillment (Steps 14-17) – Section 3.7

citi

3.1 LCMS Administrator Card Initialization (P1-P3)

3.1.1 Overview

The card initialization process sets the initial PIN on the card and prepares the cards to have PKI certificates loaded. LCMS Administration Cards are based on the Schlumberger Cryptoflex 8K card platform. The person performing this process uses the ActivCard Gold client software along with the Card Data List Utility described below to complete the card initialization.

3.1.2 Step-by-Step Process

The process should be conducted by both a "maker" and "checker" role. Please refer to ActivCard Gold documentation for more information about using and installing ActivCard Gold. For more information on the Card Data List Utility, refer to section 3.1.3.

1. The "Maker" should start the CDL utility by selecting "Start\Program\CardDataList\CardDataList." The first time the CDL utility is run it will ask for a workstation ID. Select any two alphanumerical characters to identify the workstation, possibly your initials.
2. A screen will be displayed with a randomly generated numeric PIN and two text fields. The text fields are "Unlock Code" and "Card Number".
3. Insert an un-initialized Admin card into the card reader.
4. Start the ActivCard Gold Utilities (Gold) by double clicking the smart card reader icon in the lower left corner of the Desktop.
5. Proceed with card initialization. Transfer the Card PIN from the CDL utility to Gold by typing or copy-and-paste into Gold
6. Exit and restart Gold.
7. Enter the Card PIN previously used.
8. The Unlock Code screen is displayed. Transfer the Unlock Code from the "Unlock Code" field in the CDL utility by typing or copy-and-paste into Gold.
9. Close the Unlock Code screen in Gold.
10. Select "Tools" then "View Settings" in Gold.
11. Transfer the Serial Number from the "Card Number" field in the CDL utility by typing or copy-and-paste into Gold
12. Click "Save" button on the CDL utility. A new PIN is displayed and the fields are cleared, ready for the next card.
13. Repeat the above steps for as many cards as you need to initialize.
14. To exit from the CDL utility click the close ("X") button in the upper left corner of the utility screen.
15. Exit the ActivCard Gold Utilities.
16. Every time the CDL utility is run it creates a new data file. The file is located in the "c:\CDL Files" directory and its name is "CDLyy###.txt". Where:
    - yy is the workstation ID created when CDL utility was run for the very first time,

citi

- ### is a sequential number incremented every time the utility is run.

17. The "Checker" should verify the data captured in the Card Data List. Select a card and note its ID (printed on the back). Find the associated entry for that card in the CDL.
18. Insert the card into the card reader. Start the ActivCard Gold Utilities (Gold) by double clicking the smart card reader icon in the lower left corner of the Desktop.
19. Enter the PIN listed in the CDL. The Unlock Code screen is displayed.
20. Compare the Unlock Code listed in the CDL with the one displayed. They should be the same. It is VERY important to ensure these codes match.
21. Click on "Disable Unlock Code display". This will prevent the Unlock Code from ever being displayed again. Close the screen.
22. Exit the ActivCard Gold Utilities
23. Send the initialized cards to the Arterium Security Administrator.
24. Send the associated Card Data List via signed and encrypted e-mail to the Arterium Security Administrator

A log file are maintained for auditing purposes. The log file name is "CDLyyLog.txt", where yy is the workstation ID created when CDL utility was run for the first time. The log file is stored in two locations. One is in the "c:\CDL Files" directory and another is located in the "d:\CDL Backup Files" directory.

3.1.3 Card Data List Utility

The Card Data List (CDL) utility is used to capture the initialization data for LCMS administration cards initialized with ActivCard Gold 1.2. The CDL utility runs on a PC workstation and is used in conjunction with Gold in a process that initializes LCMS Admin cards and captures selected initialization data by cutting and pasting.

3.1.3.1 System Requirements

The following are the hardware, software and networking requirements for the system on which the card initialization will be performed.

a) Hardware
   i) Pentium II or III class PC.
   ii) 64 MB RAM minimum.
   iii) Two hard disk drives.
   iv) 100 MB available space on hard drive "C:".
   v) 5 MB available space on hard drive "D:".
   vi) Standard peripherals: display, keyboard, etc.
   vii) Serial and parallel ports.
   viii) ActivCard Gold PCSC compliant serial port card reader.
   ix) Ethernet adapter.
b) Software
   i) NT 4.0 with SP 4.0
   ii) ActivCard Gold 1.2 C2.
   iii) Email client with Pretty Good Protection (PGP).

citi

iv) CCAT CDL Utility.

c) Communications
   i) LAN connection for:
   ii) Internet email.

3.1.3.2 Card Data List Utility Description

The Card Data List (CDL) utility is used to capture the initialization data for LCMS administration cards initialized with ActivCard Gold 1.2. It performs the following functions:

i) Generates CDL
   (1) Created in same folder with CDL util.
   (2) Unique name every time a new CDL is created.
   (3) CDL contains multiple card init data records.
      (a) One record per card.
         (i) Each record has multiple fields.
         (ii) Each field has a name part and a data part
         (iii) Fields:
            1. PIN: randomly generated by CDL util, numeric characters, length of four.
            2. Unlock code: pasted by operator.
               a. Length should be checked. Notify operator if not correct.
               b. Checked against previous to insure new paste. Notify operator if correct.
            3. Card number: pasted by operator.
               a. Length should be checked. Notify operator if not correct.
            4. Name (of cardholder): pasted by operator of Issuing Workstation (at eCiti Hosting)

ii) Generates log file
   (1) Single log file created in same folder with CDL util.
   (2) Backup maintained in a separate folder.
      (a) Folder location should be settable by some TBD mechanism.
   (3) Data from each CDL record is logged.
      (a) Date and time added to each record.

iii) Operates interactively
   (1) Creates new CDL at startup.
   (2) GUI for accepting record data.
   (3) Does field checks.
   (4) Writes to CDL and log upon command (i.e. button) by operator.
   (5) Exits upon command from operator.

3.1.3.3 Installing the CDL Utility

1. Install ActivCard Gold 1.2 and the card reader according to vendor instructions.

2. From the CDL Utility distribution media, run setup.exe". Follow the prompts to install the CDL utility. It will be installed under "Program Files" directory in the "CardDataList" subdirectory

3.1.3.4 Card Data List Utility Un-installation

From "Control Panel" select "Add/Remove Program" and then select "CardDataList". Follow prompts to remove CDL utility from computer.

Note: The "c:\CDL Files" and "d:\CDL Backup Files" are not removed by uninstall process. You have to remove those directories and/or files in those directories manually if needed.

citi

3.1.3.5 Building the CDL Utility

Visual Studio 6.0 and Visual Basic 6.0 are required to build CDL Distribution Pack. The following steps need to be preformed:

1. Select "Start" and "Programs" and "Microsoft Visual Studio 6.0" and "Microsoft Visual Studio 6.0 Tools" and "Package and Deployment Wizard"
2. Start "Package and Deployment Wizard"
3. Select project "C:\CardDataList\CardDataList.vbp"
4. Click on "Package" button
5. Select Package type to be "Standard Setup Package".
6. Click "Next", "Next", "Yes", and "Next".
7. Add "Citi'gif" and "pin.mdb" files in included files list.
8. Click "Next".
9. Select "Single CAB"
10. Click "Next" a few times until you will see "Finish".
11. Click "Finish".
12. Click "Save Report" and "Close"
13. Click "Close" one more time.
14. The Distribution CD is in the "c:\CardDataList\Package" directory. The distribution files are "Setup.exe', Setup.lst", and "CDL.cab".

3.2 LCMS Administrator Card Receipt and Storage (Steps P4-P6)

3.2.1 Overview

The Arterium Security Administrator receives the LCMS Administration Cards and associated Card Data List. The administrator should notify the Issuing Workstation Operator of the receipt of the cards, and document log the receipt of the cards for change control purposes. It is then the responsibility of the Issuing Workstation Operator track the inventory of cards and securely store the information until new cards need to be personalized.

3.2.2 Step-by-Step Process

1. The Arterium Security Administrator receives the Card Data List via signed and encyrpted e-mail from the Card Initializer.
2. The Arterium Security Administrator receives the initialized LCMS Admin Cards via shipment
3. Verify the CDL information matches the card shipment by verifying it has the correct number and IDs of the cards.

4. Log the receipt of the cards and notify the Card Initializer the information is correct

5. Send the CDL to the Issuing Workstation Operator via signed and encrypted e-mail and send the cards in a separate package.

6. The Issuing Workstation Operator should store the CDL and initialized LCMS Admin Cards securely until ready for use

7. The Arterium Security Administrator should track to make sure the number of LCMS Admin Card requests coming in does not exceed the inventory of cards available. As the inventory depletes, notify the Card Initializer that more cards are required.

3.3 Account Request and Approval (Steps 1-3)

3.3.1 Overview

The Program Administrator is responsible for issuing new account requests. These requests can be for new LCMS Admin Card accounts, UID/Password accounts, or System User accounts. The Program Administrator gathers the required account request data and submits the Account Request file via secure e-mail to the Citibank Business Manager. The Business Manager is responsible for reviewing and approving the access request. The Business Manager then sends the approved request via secure e-mail to the Arterium Security Administrator for processing.

3.3.2 Step-by-Step Process

1. The Program Administrator generates the Account Request File and sends to the Citibank Business Manager using signed and encrypted e-mail.

2. The Business Manager should reviewed the ARF for the following items:

- Determine if the requested access is approved
- Determine if the ARF is complete and in the correct format

3. The Business Manager should inform the Program Administrator should be informed of any mistakes and the Program Administrator should correct and re-submit the ARF if necessary.

4. If the format is correct and the Business Manager deems the request to be acceptable the ARF should be sent via signed and encrypted e-mail the Arterium Security Administrator.

3.3.3 Account Request File Requirements

The ARF is used for LCMS Admin Card requests, UID/password requests, and system user requests. These requests can either be to add or delete an account. The ARF should only be sent using encrypted and signed e-mail.

LCMS Account Request File Requirements
==========

Text file(s) should be submitted with the following format:

a(add)/d(delete);first name;last name;userid;e-mail address;role
a(add)/d(delete);first name;last name;userid;e-mail address;role
a(add)/d(delete);first name;last name;userid;e-mail address;role

For example:

a;joe;smith;jsmith1;joe.smith@company.com;sunHelpDeskOfficer
a;kim;jones;;kim.jones@company.com;sunAdminOfficer
a;tom;wilson;tom wilson;tom.wilson@company.com;sunAdminOfficer
a;joe k.;smith;jsmith2;joe.k.smith@company.com;sunHelpDeskOfficer
a;sunserver.sun.com;;;administrator@sun.com;activCardServer

NOTE: Separate files should be created for "adds" vs. "deletes" due to security risks in processing account deletions in a timely manner.

Notes about format/content of data
==========

- All information except the role name is not case sensitive
- Specify an "a" at the beginning of the record for an add, and a "d" for a delete. If records should be modified, first specify that the record be deleted, and then specify an add record with the updated information
- The roles are either sunAdminOfficer, sunHelpDeskOfficer, citiAdminOfficer, Vendor, hostingAdminOfficer, activCardServer or badgingStation. These role names are case sensitive.
- For those with the sunAdminOfficer, citiAdminOfficer, Vendor activCardServer and badgingStation role the UserID field should be left blank. For example:

  a;Joe;Smith;;joe.smith@company.com;sunAdminOfficer

  This role does not have to enter the user ID because it is automatically stored on the Admin card and generated based on a combination of the first and last name.

- For those with the sunHelpDeskOfficer or hostingAdminOfficer role, the UserID field can be populated with the desired login ID. There are no character limitations to this field, but it must be unique across all users. If this field is left blank, then by default the user will be assigned a UserID that is equal to their Common name, or the combination of their first and last name. For example:

  a;Joe;Smith;jsmith1;joe.smith@company.com;sunHelpDeskOfficer - Joe's login ID would be jsmith1
  a;Joe;Smith;;joe.smith@company.com;sunHelpDeskOfficer - Joe's login ID would be Joe Smith

- Across ALL users (regardless of role), the Common name, or the combination of their first and last name, MUST be unique. If there is more than one user with the same first and last name, add an initial or a unique character to the first name field to distinguish the names apart. For example:

  a;Joe;Smith;;joe.smith@company.com;sunAdminOfficer
  a;Joe W.;Smith;;joewsmith@company.com;sunAdminOfficer

- For System users, the First Name field should be used to specify the System hostname. The Last name field should be left blank. The e-mail address should be the e-mail address of the server system administrator. The role for the Sun ACMS and Portal is "activCardServer". The role for the Sun Badging Station is "badgingStation". For example:

  a;sunserver.sun.com;;;administrator@sun.com;activCardServer

- The e-mail address provided for those users getting an LCMS Admin Card or System User certificate will be the e-mail address to which the certificate renewal notification is sent when the certificate expires. It is important to use an active e-mail address so that the proper user will receive and act on the renewal notice.

3.4 Account Request File Processing (Steps 4-7)

3.4.1 Overview

The Arterium Security Administrator is not responsible for approving access requests to Arterium. This responsibility lies with the Business Manager. Once the Arterium Security Administrator receives the signed and encrypted ARF from the Business Manager, this means the requests have been approved and are ready for processing. The Arterium Security Administrator should review and log the account requests, and then send the reviewed file to the LDAP Operator for import into the Arterium LDAP directory.

The ARF is an abbreviated form of an LDIF file. The ARF must be converted to a full LDIF file before it can be imported into the LDAP system, to create accounts for pre-authorized users. The LDIF File Generator utility is used to create the full LDIF file. In addition the LDIF File Generator will produce a second file, the one-time-use PIN Creation List (PCL). This one-time-use PIN is required to perform the download of the approved certificate.

The LDIF file created by the LDIF File Generator utility must be imported into the LDAP to create the accounts for pre-authorized users.

3.4.2 Step-by-Step Process

1. The Arterium receives the approved Account Request File via signed and encrypted e-mail from the Citibank Business Manager
2. The request should be logged for a later check on the number of accounts issued.
3. Although the Business Manager should have already examined the ARF for correct formatting, verify the ARF is properly formatted.

citi

4. For those request for UID/password based accounts (sunHelpDeskOfficer, hostingAdminOfficer), amend each account request with a password. Choose a password that complies with Citibank security policies (at least 8 characters, must contain upper and lower case alpha and a numeric character).

   For example, if the entry says this:

   ```
   A;Fred;Pinn;FredAPinn;fred.pinn@sun.com;SunHelpDeskOfficer

   Append the entry to read like this:

   A;Fred;Pinn;FredAPinn;fred.pinn@sun.com;SunHelpDeskOfficer;Helpdesk1

   Where "Helpdesk1" is the password for that account.
   ```

5. For all other roles, amend the entry with the password "citibank". For these roles, this password will not be used for user authentication to Arterium but is a required field in order to complete the access request process.

6. Send the reviewed and updated ARF to the LDAP Operator via signed and encrypted e-mail for further processing.

7. The LDAP Operator receives the ARF via signed and encrypted e-mail from Arterium Security Administrator.

8. Run the LDIF File Generator Utility, using the ARF as the Input file. Place the ARF file(s) in the same directory (on LDAP machine) as the Perl script and execute the following command:

   perl Ascii2Ldif.pl <input file> <organization>

   The first parameter, <input file> is the name of the ARF containing the semicolon-delimited data. The second parameter <organization> is the organizational name. If not supplied, then it defaults to 'Citibank'.

9. Compare the .LOG file to the ARF to verify the correct number of accounts have been added, deleted or modified and view the LDAP directory entries to make sure the correct actions were actually taken.

10. View the REMAINDER file to see if there are any simple format errors in the records that can be corrected and re-run. If so, make the corrections to those records and run these corrected records through the LDIF File Generator Utility, using the corrected records as the Input file

11. If there are errors for duplicate names, incomplete information, etc. pass these records back to the Arterium Security Administrator for follow-up.

12. Import the LDIF file into the LDAP directory using the Directory Server Console.

13. Run the PIN Creation List (PCL) file through the Netscape PIN Generation Utility. To do this, execute the following command at the command prompt:

    ```
    setpin host=<hostname>.com port=389 "binddn=CN=Directory Manager"
    bindpw=DMpasswd "filter=(uid=*)" basedn=o=CDCLA, c=US input=inputfile
    output=/tmp/pin.log write
    ```

14. Send the output file of the PIN Generation Utility via signed and encrypted e-mail to the Issuing Workstation Operator. This output file is also called the Certificate Account List (CAL)

citi

3.4.3 LDIF File Generator Utility

This utility converts semicolon delimitated files into LDIF files. LDIF files are used to update the LDAP. The utility is actually a Perl script that requires the Perl interpreter in order to run.

3.4.4 LDIF File Generator Utility Installation

3.4.4.1 Supported Platforms

Windows 95, Windows 98, Windows NT, Solaris, Linux are all supported, as long as there is a Perl interpreter available for the platform.

3.4.4.2 Perl Installation

Perl is assumed to be installed on the platform. If not, and there is a need for Perl, the user can obtain Perl from http://www.activeperl.com The download is free and the Windows, Solaris and Linux platforms are supported. Follow the directions on the site to install the Perl package. This Perl script has been tested using version 5.6.0.623.

3.4.4.3 Script Installation

The script is installed by simply copying the script to the directory that holds the ASCII delimitated input files. The Perl script file name is "Ascii2Ldif.pl".

3.4.5 LDIF File Generator Utility Operation

3.4.5.1 Input File Syntax

The Input file is a collection of semicolon delimitated records containing user information. The general form of the Input records are:

```
<action>;<GivenName>;<SurName>;<UserId>;<EmailAddress>;<Role>;<Password>
```

or an empty line.

3.4.5.1.1 Add Record

The syntax for the Add record is as follows

```
a;<Given Name>;<Sir Name>;<User Id>;<Email Address>;<Role>
```

or

```
a;<Server Name>;;<Server Name>;<Email Address>;<Role>
```

or

```
a;<Given Name>;<Sir Name>;<User Id>;<Email Address>;<Role>;<Password>
```

Where:

'a'	is the action, Add Record.
<Given Name>	is the first name of user.
<Sir Name>	is the family name of the user.
<User Id>	is the user's login name. If this field is omitted and the role is 'sunAdminOfficer', 'citiAdminOfficer', 'Vendor', 'activCardServer', or 'badgingStation', then it is produced from the Given Name and Sir Name concatenated with a space. 'Jane' and 'Doe' would produce 'Jane Doe' as a user.
<Email Address>	is the Email Address of the user. This field is mandatory.
<Role>	is the Role of the user. It may be one of the following: 'sunHelpDeskOfficer', 'sunAdminOfficer', 'citiAdminOfficer', 'hostingAdminOfficer', 'Vendor', 'activCardServer', or 'badgingStation'. These values are not case sensitive in the input file,

	but are in the resulting LDIF file. The script will convert these values properly.
<Password>	is the password associated with the user's user id. If the password is not supplied, then for roles 'hostingAdminOfficer' and 'sunHelpDeskOfficer' the password will be randomly generated. For roles, 'sunAdminOfficer', 'citiAdminOfficer', 'Vendor', 'activCardServer', or 'badgingStation', the password 'citibank' will be the default.

3.4.5.1.2 Delete Record

The syntax for the Delete record is the same as the Add record except that the action (the first field) is always 'd', for delete. The only two fields needed for delete is the action ('d') and the user id. Trailing semicolons may be omitted.

```
d;;;<User Id>;;;
```

3.4.5.1.3 Modify Record

The syntax for the Modify record is the same as the Add record except that the action (the first field) is always 'm', for modify. The only mandatory fields for modify are the action ('m') and the user id. Trailing semicolons may be omitted.

```
m;<GivenName>;<SurName>;<UserId>;<EmailAddress>;<Role>;<Password>
```

Please remember, only the action (m) the user id and any fields to be changed are entered.

Example 1)

```
m;;;KarenPinn;KPinn@csi.com;
```

Changes user KarenPinn's email address only.

Example 2)

```
m;;;FredAPinn;;SunAdminOfficer;tOPsECREt
```

Changes user FredAPinn's role and password.

3.4.5.2 Roles

Following are the accepted roles:

- citiAdminOfficer
- hostingAdminOfficer
- sunHelpDeskOfficer
- sunAdminOfficer
- Vendor
- activCardServer
- badgingStation

PLEASE NOTE: The roles are case sensitive in the LDIF file but are not case sensitive in the INPUT file.

3.4.5.3 Running Ascii2Ldif.pl

At the command prompt type:
perl Ascii2Ldif.pl <input file> <organization>

citi

The first parameter, <input file> is the name of the file containing the semicolon delimitated data. The second parameter <organization> is the organizational name. If not supplied, then it defaults to Citibank.

Any errors encountered in parsing the input file are displayed on the screen. After all records are processed, statistics are displayed for how many records have been added, modified, deleted or rejected.

Example:

```
>perl ascii2ldif.pl UserInfo
a;Karen;Pinn;KarenPinn;KarenPinn@csi.com;sunAdminOfficer
ERROR: Common name 'Karen Pinn' has already been added.
a;Karen;Zinn;KarenPinn;KarenPinn@csi.com;sunAdminOfficer
ERROR: UID 'KarenPinn' has already been added.
a;Max;Pinn;;Max@pets.com;funAdminOfficer
ERROR: Role funAdminOfficer not defined.
A;Elton;Lin;;elton.lin@citicorp.com;SunHelpDeskOfficer
ERROR: UID is not specified.
m;;;FredAPinn;;ZunAdminOfficer
ERROR: Role ZunAdminOfficer not defined
v;;Blah
ERROR: Action 'v' must be either 'a', 'm', or 'd'
Number of records added ..... 2
Number of records modified ..... 2
Number of records deleted ..... 1
Number of records rejected ..... 6
Number of blank records ..... 2
Total number of records processed ..... 13
```

3.4.5.4 Files Used and Produced

There are up to four files generated by the Ascii2Ldif.pl perl script. The LDIF file, LOG File, PIN file, and the REMAINDER file (*only if there are errors*). The INPUT file is a file with no extension. The generated files have the same name as the INPUT file with the extensions ".ldif", ".log", ".pin" and ".remain".

Given an input file called 'UserInfo', the files 'UserInfo.ldif', 'UserInfo.log', 'UserInfo.pin', and possibly 'UserInfo.remain' will be created.

Example INPUT File containing errors:

```
a;Karen;Pinn;KarenPinn;KarenPinn@csi.com;sunAdminOfficer
a;Karen;Pinn;KarenPinn;KarenPinn@csi.com;sunAdminOfficer
a;Karen;Zinn;KarenPinn;KarenPinn@csi.com;sunAdminOfficer
a;Max;Pinn;;Max@pets.com;funAdminOfficer

A;Fred;Pinn;FredAPinn;pinn@cdcla.com;SunHelpDeskOfficer;topSecret
A;Elton;Lin;;elton.lin@citicorp.com;SunHelpDeskOfficer

m;;McCarthy;KarenPinn;McCarthy@csi.com;
m;;;FredAPinn;;ZunAdminOfficer
m;;;FredAPinn;;SuNHelpDeskOfficer
v;;Blah
d;;;FredAPinn;;
```

The errors are listed in the example shown in *"Running Ascii2Ldif.pl"* (above).

citi

3.4.5.4.1 LDIF File

The LDIF File is the file that is used to update the LDAP. Once this LDIF file is generated, it then needs to be imported into the Directory Server (LDAP) database.

Example of a LDIF file produced by the above INPUT file.

```
dn: uid=KarenPinn, o=Citibank, c=US
changetype: add
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: artPerson
cn: Karen Pinn
givenname: Karen
sn: Pinn
uid: KarenPinn
mail: KarenPinn@csi.com
role: sunAdminOfficer
iphostnumber: *
defaultpartition: sun
userpassword: citibank

dn: uid=FredAPinn, o=Citibank, c=US
changetype: add
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: artPerson
cn: Fred Pinn
givenname: Fred
sn: Pinn
uid: FredAPinn
mail: pinn@cdcla.com
role: sunHelpDeskOfficer
iphostnumber: *
defaultpartition: sun
userpassword: topSecret

dn: uid=KarenPinn, o=Citibank, c=US
changetype: modify
replace: sn
sn: McCarthy
-
replace: mail
mail: McCarthy@csi.com
-
replace: userpassword
userpassword: citibank

dn: uid=FredAPinn, o=Citibank, c=US
changetype: modify
dn: uid=FredAPinn, o=Citibank, c=US
changetype: modify
replace: role
role: sunHelpDeskOfficer
-
replace: userpassword
userpassword: citibank

dn: uid=FredAPinn, o=Citibank, c=US
changetype: delete
```

citi

3.4.5.4.2 LOG File

The LOG file shows all processed records with any error messages associated with the conversion. Any records that have listed errors will not be processed and put into the LDIF file. These records will be placed in the REMAINDER file discussed in the following section.

LOG File Example:

```
1) a;Karen;Pinn;KarenPinn;KarenPinn@csi.com;sunAdminOfficer
2) a;Karen;Pinn;KarenPinn;KarenPinn@csi.com;sunAdminOfficer
ERROR: Common name 'Karen Pinn' has already been added.
3) a;Karen;Zinn;KarenPinn;KarenPinn@csi.com;sunAdminOfficer
ERROR: UID 'KarenPinn' has already been added.
4) a;Max;Pinn;;Max@pets.com;funAdminOfficer
ERROR: Role funAdminOfficer not defined.
5) <blank>
6) A;Fred;Pinn;FredAPinn;pinn@cdcla.com;SunHelpDeskOfficer;topSecret
7) A;Elton;Lin;;elton.lin@citicorp.com;SunHelpDeskOfficer
ERROR: UID is not specified.
8) <blank>
9) m;;McCarthy;KarenPinn;McCarthy@csi.com;
10) m;;;FredAPinn;;ZunAdminOfficer
ERROR: Role ZunAdminOfficer not defined
11) m;;;FredAPinn;;SuNHelpDeskOfficer
12) v;;Blah
ERROR: Action 'v' must be either 'a', 'm', or 'd'
13) d;;;FredAPinn;;
```

3.4.5.4.3 REMAINDER File

The remainder file contains the input records that could not be processed due to syntactical errors or are duplicate additions. These records can be edited and reprocessed as a new input file. The REMAINDER file has the extension '.remain'.

Example from the same run as the above LOG file:

```
a;Karen;Pinn;KarenPinn;KarenPinn@csi.com;sunAdminOfficer
a;Karen;Zinn;KarenPinn;KarenPinn@csi.com;sunAdminOfficer
a;Max;Pinn;;Max@pets.com;funAdminOfficer
A;Elton;Linn;;elton.lin@citicorp.com;SunHelpDeskOfficer
m;;;FredAPinn;;ZunAdminOfficer
v;;Blah
```

3.4.5.4.4 PIN Creation List (PCL) File

The PCL file contains the domain designations of added records.

Example PCL file using the above INPUT file:

```
dn: uid=KarenPinn, o=Citibank, c=US

dn: uid=FredAPinn, o=Citibank, c=US
```

This PCL file is used as an input file for the one-time-use PIN Generation Utility. The file specifies to the PIN Generation Utility which of the users in the LDAP database require PINs. The use of the PIN Generation Utility is described below.

3.4.5.5 Error Codes

Following is a list of Error Codes for Ascii2Ldif.pl:

```
ERROR: Action 'v' must be either 'a', 'm', or 'd'
ERROR: Common name 'Karen Pinn' has already been added.
ERROR: Email is not specified.
ERROR: Role funAdminOfficer not defined.
ERROR: UID 'KarenPinn' has already been added.
ERROR: UID is not specified.
```

3.4.6 LDAP Import

The Directory Server Console can be used to import the LDIF file into the directory server database. For best performance, the server console should only be used to import an LDIF file only if the LDIF file contains a relatively small number of directory entries (less than 10,000). Otherwise, command-line utilities should be used. NOTE: since LDIF files imported via command-line will overwrite any existing database entries, it is not recommended.

To import LDIF using the Directory Server Console:

1. On the Directory Server Console select the 'Configuration' tab.
2. From the Console menu, select 'Import'. This displays the Import Database dialog box.
3. Enter the full path to the LDIF file in the field provided. To search for the file, click 'Browse'.
4. Select "Append Data to Database" as the import method. When importing with this option, the server does not delete the contents of the directory before adding the entries from the LDIF file.
5. Select "Continue on Errors" to allow the import to continue even if it encouters duplicates.
6. Click OK and the server performs the import. Any rejected entries will appear in the file specified in the 'File for rejects' field.

3.4.7 PIN Generation Utility

Once the LDIF file has been imported successfully into the database, the PIN Generation Utility that is included with the Netscape Certificate Management System can be executed, using the .PIN file as an input. The PIN Utility adds a random 6-digit PIN to the LDAP entry for each user specified in the PIN file. The PIN Utility outputs a file (genpin.log) that lists the selected users and their respective random PINs. Using this list, as well as the LOG file (described above), generating/retrieving certificates from the RA using username/password/PIN can then proceed.

The PIN Generator is located on the Registration Authority (RA) server at `<server_root>/bin/cert/tools/setpin`, where `<server_root>` is the directory where the CMS binaries are kept. The command line is as follows:

```
/usr/netscape/ra/bin/cert/tools/setpin host=LDAPhostname
port=port "binddn=CN=Directory Manager" bindpw=password
"filter=(search_criteria_ie_ uid=*)"
basedn=o=organization_name,c=US input=file_of_DNs_to_process
output=outputfile write
```

citi

The following command generates PINs for all entries that have the `uid` attribute (in their distinguished name) defined in an LDAP directory on a server called `javabadge1.tti.com` that is listening on port `389` (default LDAP port). The PIN Generator binds to the directory as user `Directory Manager` and starts searching the directory from the node `dn=o=CDCLA, c=US` in the directory tree. The tool specifically searches for the DNs listed in the input file `inputfile`. Any LDAP entry that is not specified in `inputfile` is ignored. The tool does not overwrite existing PINs.

```
setpin host=javabadge1.tti.com port=389 "binddn=CN=Directory
Manager" bindpw=DMpasswd "filter=(uid=*)" basedn=o=CDCLA, c=US
input=inputfile output=/tmp/pin.log write
```

This utility will generate a log file (as specified in '`outputfile`') with the following format.

```
dn: <user_dn>1
pin: <generated_pin>1
status: <status>1
<blank line>
dn: <user_dn>2
pin: <generated_pin>2
status: <status>2
...
dn: <user_dn>n
pin: <generated_pin>n
status: <status>n
```

where `<user_dn>` is a distinguished name that matched the specified DN pattern (specified by the '`filter`' option).
`<generated_pin>` is a string of characters
`<status>` is '`added`' if the pin has been added, '`replaced`' if the PIN has been replaced ('`clobber`' option must be specified in command line), or '`notreplaced`' if the old PIN was not replaced ('`clobber`' option was not specified).

The following is an example of the output file that is generated. If an input file is used, the output file will only display the PINs generated for the users specified in the file.

```
dn:uid=SunAdmin1, o=Citibank, c=US
pin:ldg7fy
status:added

dn:uid=SunHelpDesk1, o=Citibank, c=US
pin:fmZI8w
status:added

dn:uid=joker, o=Citibank, c=US
pin:elrAm9
status:added
```

citi

3.5 LCMS Administrator Card Personalization (Step 8-9)

3.5.1 Overview

The personalization step includes downloading a PKI certificate for an approved user to the initialized LCMS Admin Card. This certificate will allow the user to login to the LCMS. The personalization step begins when the Certificate Account List (CAL) is sent by the LDAP Operator and contains the account (i.e. "dn" field) and one-time-use PIN data for accessing web-based accounts that will personalize the cards. This list shows the total number of cards that need to be created.

A Card Issuing Workstation is required to personalize the LCMS Admin Cards. The Issuing Workstation has a smart card subsystem product installed on it, as well as the Netscape browser. The smart card subsystem includes software and a card reader. When the smart card subsystem is installed it also adds the ability for the Netscape browser to interact with smart cards. The card reader and browser are used to personalize the card. The Issuing Workstation Operator will personalize cards on behalf of the cardholders.

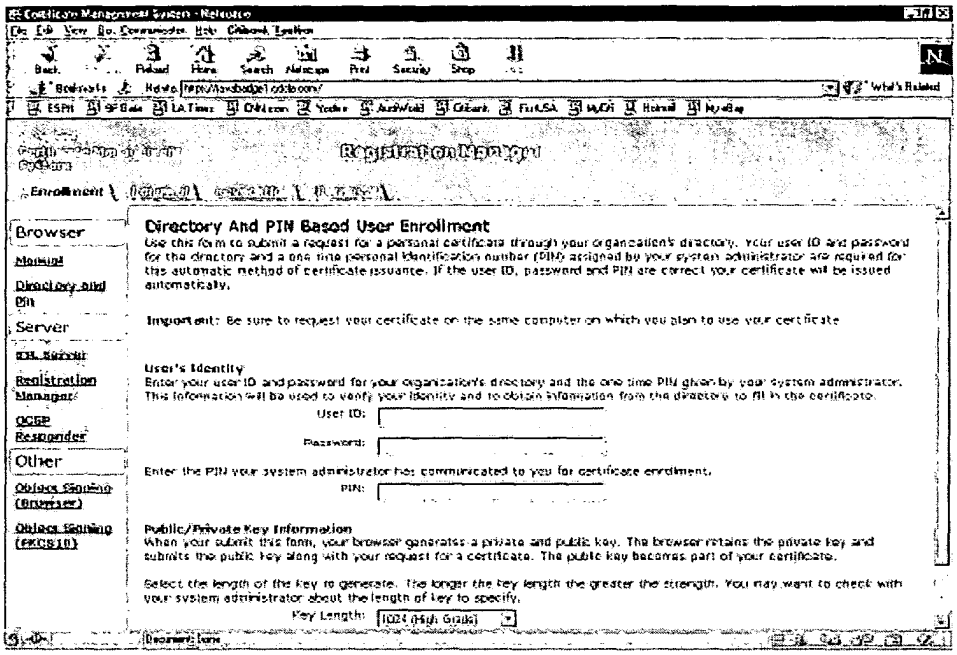
NOTE: There are two "PINs" referenced in this section. The card PIN, listed in the CDL, is used to access the LCMS Admin Card. The one-time-use PIN, listed in the CAL, is used as authorization to the RA Website when performing the download of the certificate to a particular card.

Using the Netscape browser and the ActivCard client software on the Issuing workstation, complete the process to add certificates to the required LCMS Admin cards. When the process is complete e-mail the Activated Card List to the Arterium Security Administrator for verification.

3.5.2 Step-by-Step Process

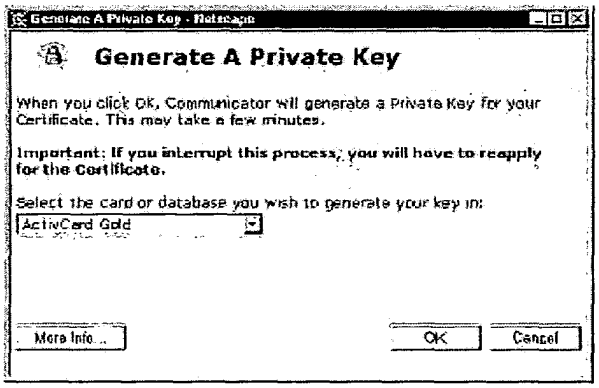
1. Receive the initialized LCMS Admin Cards and the Card Data List (CDL) via secure e-mail from the Arterium Security Administrator
2. Store the cards and the CDL in a secure locked location until ready to personalize the cards
3. Receive the Certificate Account List via secure e-mail from the LDAP Operator
4. Review the CAL to determine how many cards need to be personalized and retrieve the appropriate number of LCMS Admin Cards from secure storage. Also retrieve the CDL information for those cards
5. Make a copy of the CDL onto the Issuing Workstation. Name it "ACLmmddyy.txt", where mmddyy is the date. This will be the Activated Card List when it has been properly edited.
6. Access the RA Web site from the Netscape Browser on the Issuing workstation. On an issuing workstation, go to https://www.cardmanagement.citibank.com:8144.
7. Click on 'Directory and Pin'
8. Submit the LCMS card to be personalized into the card reader.
9. At the enrollment page, enter the user ID, password (citibank), and PIN (from the Certificate Account List) the click Submit.

citi



10. User will then be prompted for card pin (original issued card pin). Reference the CDL created previously for the card's ID number, printed on the back of the card. Type in card pin and press 'Enter'.

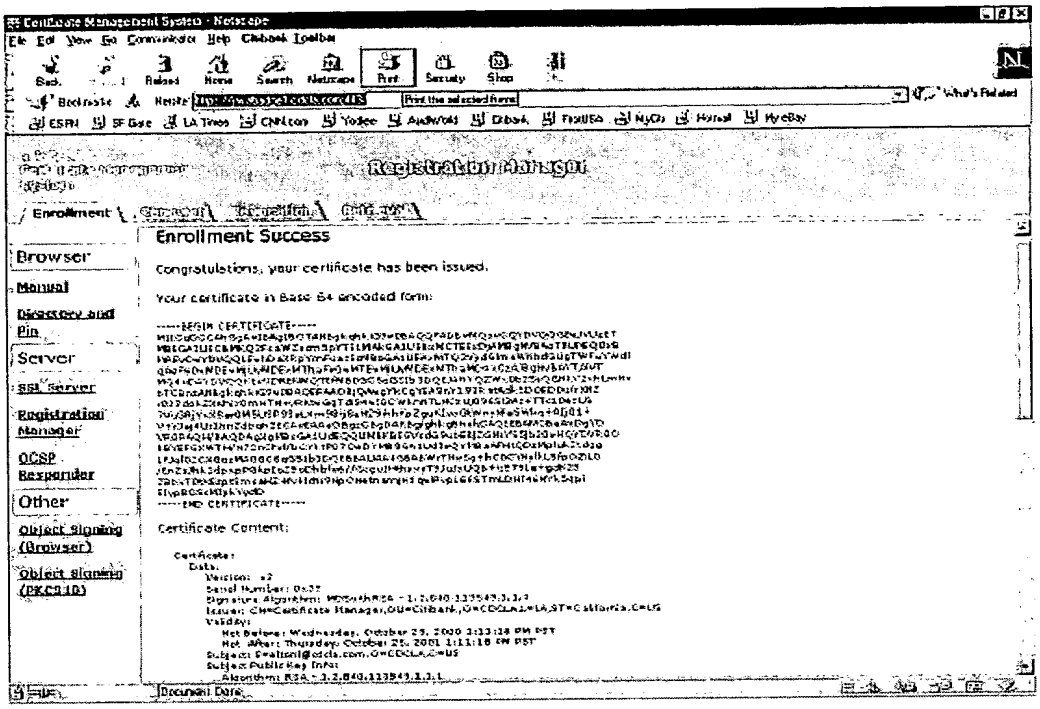
11. Once this information is submitted, a key pair is generated on the card. This key pair will not be usable until a valid signed certificate is imported



12. After the key pair is generated, the RA automatically verifies the userid, password, and PIN information with the information stored in the LDAP database. If the userid, password, and PIN match, the request is automatically approved by the RA and sent to the CA for signing

13. The CA then sends the signed certificate back to the RA and the detailed information displayed to the user. At the same time, the certificate is sent to the user and automatically imported onto the card. When the process completes, you will see the following message:

citi



14. Enter the user's User ID associated with the card into the "Name" column of the Card Data List. With this information the file is now called the "Activated Card List"

15. Verify the certificate download completed correctly by viewing the card contents via the ActivCard Gold utilities. Follow these steps:

    - Insert the LCMS Admin Card into card reader
    - Click on ActivGold icon, which is located on the lower right tool bar on the Desktop.
    - When prompted to enter the card pin (which is found in the CDL file), enter the pin and then click 'OK'.
    - If a window displaying the card's unlock code appears, click 'Close' on that window.
    - The main 'ActivCard Gold Utilities' window should now be displayed. Click on the 'Certificates' tab.
    - If the certificate was successfully downloaded to the admin card, it will be listed.
    - To escape the ActivGold utility window, click 'Cancel'.

16. Repeat the process above for each LCMS Admin Card to be created.

17. Send the Activated Card List to the Arterium Security Administrator using signed and encrypted e-mail. In the body of the e-mail indicate the number of cards personalized and dates when the first card and last cards were personalized (if personalization took place over a number of days). This will be used to confirm that the correct number of certificates was issued.

citi

3.5.3 ActivCard Gold Reset Utility

If for some reason the card personalization process does not complete correctly, the card can be deleted and the process repeated. The ActivCard Gold 'Reset' utility allows the user to clear all current users and data from an LCMS Admin Card and reset it so that new users can be loaded onto it. (Note: In most cases, the PIN utility would have to be re-run before downloading a new certificate onto the card.) The following steps outline utilizing the 'Reset' utility on a card:

1. On the issuing workstation, insert the LCMS Admin Card into the card reader.
2. Find the agreset application file located in the ProgramFiles\ActivCard\ActivCard Gold\ directory on the issuing workstation.
3. Click on agreset file. 'ActivCard Gold Reset' window appears.
4. Select the 'PIN' radio button, if it is not already selected. Enter the card's PIN (found in the CDL file). Click 'Reset'.
5. A window will appear stating 'Are you sure you want to reset card?' Click 'Yes'.
6. Another window will appear stating 'Card successfully reset'. Click 'OK'.
7. Click 'Close' on the main 'ActivCard Gold Reset' window.
8. Click on ActivGold icon, which is located on the lower right tool bar on the Desktop.
9. 'ActivCard Gold Utilities' window will appear stating 'Your card is not initialized. Do you want to initialize it now?' Click 'Yes'.
10. An 'Initialize Smart Card' window now appears asking user to enter and confirm a new pin. Enter the PIN that was designated for that card in the Card Data List. Click 'Initialize Smart Card' button.
11. 'ActivCard Gold Utilities' window will appear stating 'The Smart Card initialization was successfully completed.' Click 'OK'.
12. To escape the 'ActivCard Gold Utilities' utility, click 'Cancel' on this window.

3.5.4 Issuing Workstation System Requirements

1) Hardware
   a) Pentium II or III class PC.
   b) 64 MB RAM minimum.
   c) 100 MB available hard disk space.
   d) Standard peripherals: display, keyboard, etc.
   e) Serial and parallel ports.
   f) Ethernet adapter.
   g) ActivCard Gold PCSC compliant serial port card reader.
2) Software
   a) NT 4.0 with SP 4.0
   b) ActivCard Gold 1.2.1
   c) Netscape Communicator, ver. 4.X.
   d) Email client with Pretty Good Protection (PGP).
3) Communications
   a) LAN connection for:
      i) LCMS CA web site access.

ii) eCiti Hosting's internal email.

4) Special setup
   a) Create folder "C:\ACL Files".

Contains Activated Card Lists.

3.6 LCMS Administrator Card Confirmation and Delivery (Steps 10-13)

3.6.1 Overview

The Arterium Security Administrator needs to perform the "checker" role of the LCMS Admin Card creation process. Once the Security Administrator has verified the proper number of new certificates and cards were created, he gives the OK to the Issuing Workstation Operator to mail the personalized LCMS Admin Cards to the requesting organization Program Fulfillment person. As a separate message, the Arterium Security Administrator sends the Activated Card List to the requesting organization Program Administrator.

3.6.2 Step-by-Step Process

1. The Arterium Security Administrator should compare the information in the Activated Card List to the original Account Request File to ensure the proper number of cards was created.

2. Use the Agent Services of the Netscape CMS to list the certificates created by date. Verify the proper number of certificates was created. Please see the "Agent Services" page for the "Certificate Manager" in the "Netscape CMS Administrator's Guide" for instructions on how to list certificates by date.

3. Upon verification, the Arterium Security Administrator gives the OK to the Issuing Workstation Operator to distribute the new LCMS Admin Cards

4. The Issuing Workstation Operator sends the cards in bulk to the requesting organization Program Fulfillment contact.

5. The Arterium Security Administrator sends the Activated Card List via signed and encrypted e-mail to the requesting organization Program Administrator.

3.7 LCMS Administrator Card Fulfillment (Steps 14-17)

3.7.1 Overview

The fulfillment task for new LCMS Administrator Cards is designed for two separate roles: the Program Administrator and Program Fulfillment. Separating these duties ensures that no one person has both the physical cards, with the card PINS, before the rightful owner of the card receives it. Program Fulfillment is responsible for physical card distribution, and Program Administration is responsible for card PIN distribution and unlock code archival.

3.7.2 Step-by-Step Process

1. The Program Administrator receives the Activated Card List from the Arterium Security Administrator via signed and encrypted e-mail.

2. The ACL data should be securely archived so that if a user ever locks their card, they can contact the Program Administrator to obtain the unlock code.

3. The Program Administrator should securely distribute the card PIN to the correct end user.

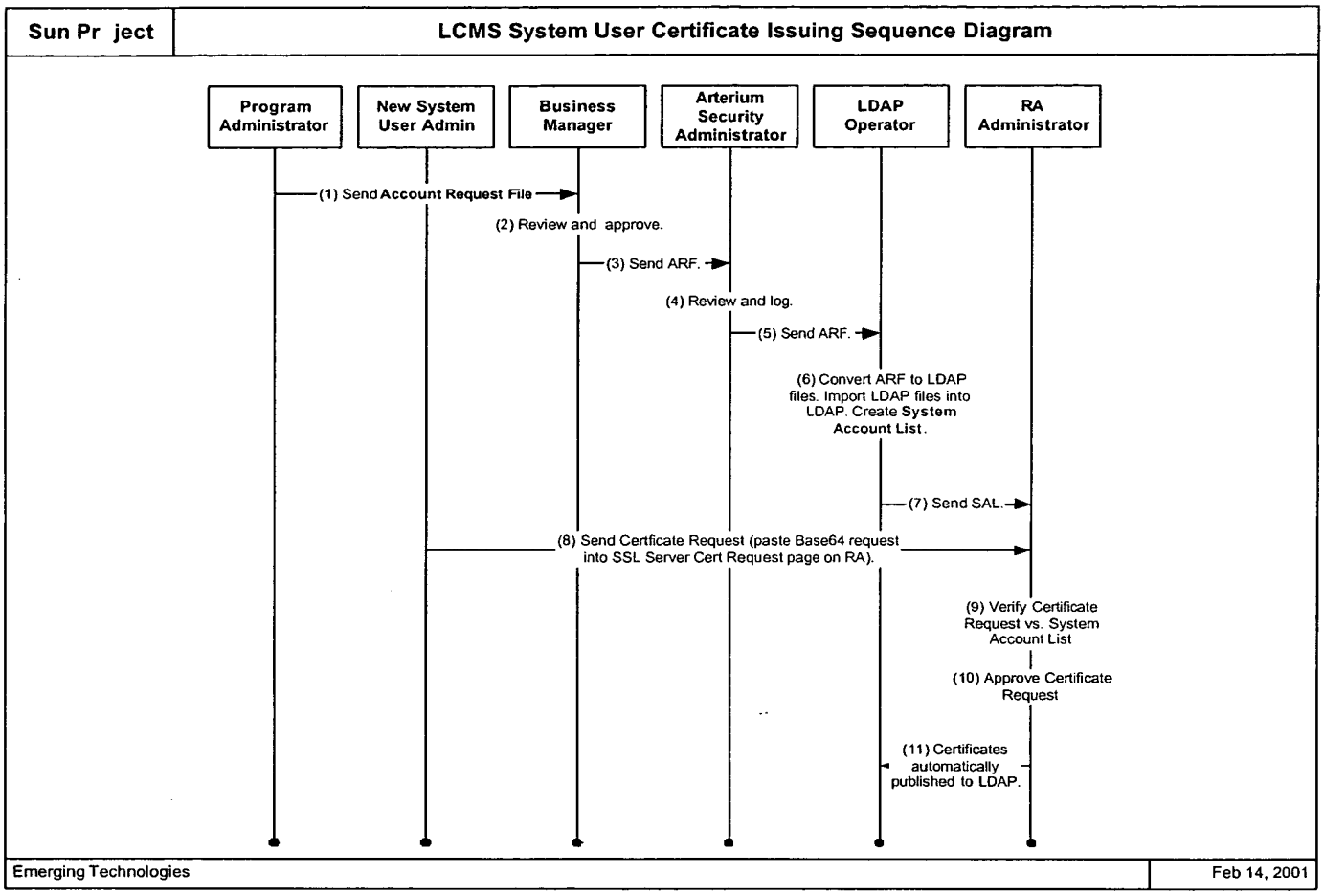
4. Program Fulfillment will receive the shipment of new LCMS Admin Cards from the Issuing Workstation Operator.

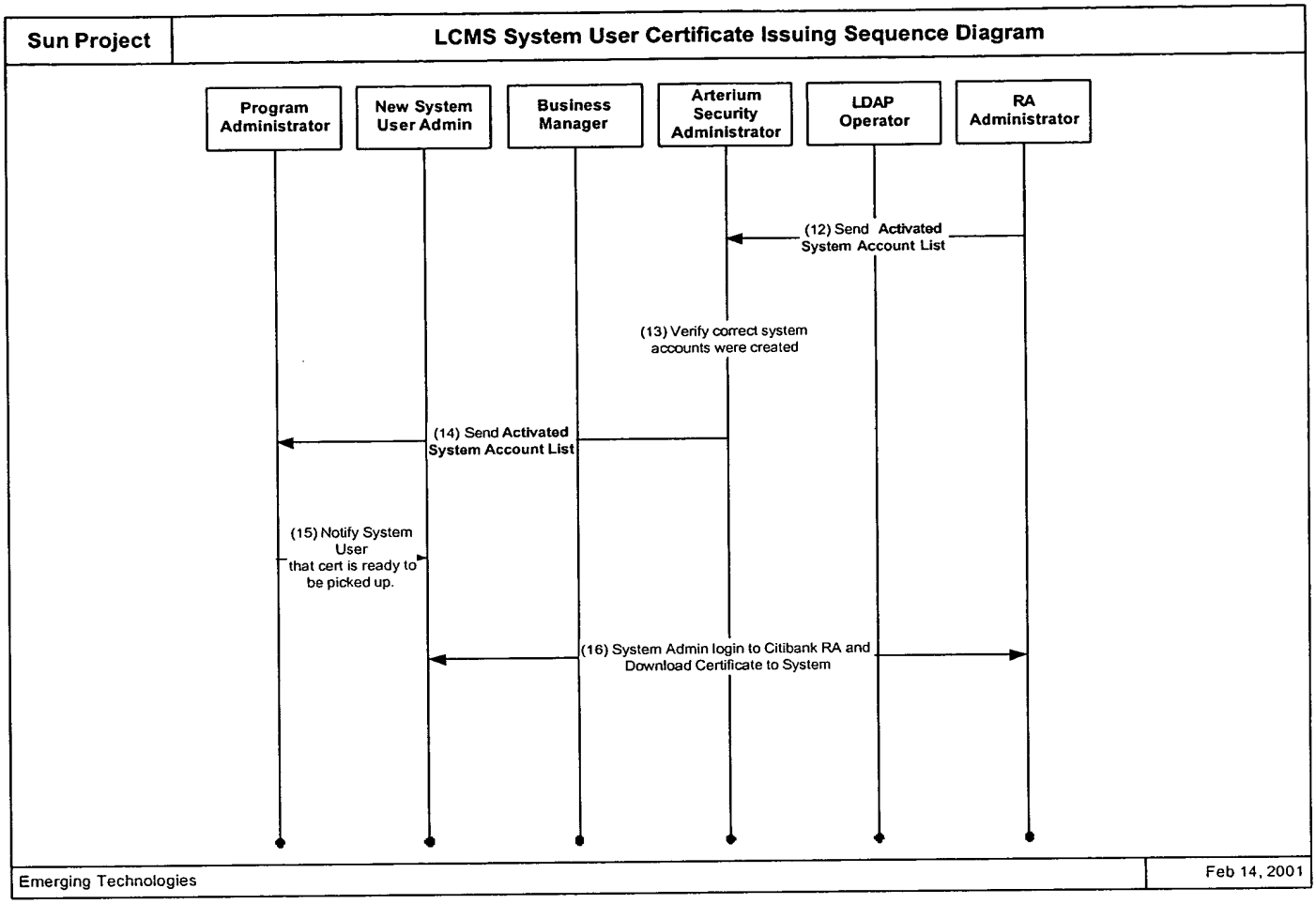
5. The new LCMS Admin Cards should be sent to the correct user once they have received their new card PIN.

citi

4 LCMS System User Certificate Issuing Process

The following diagram shows the overall process for LCMS System User Certificate Issuance. Each of the steps and the utilities and programs required to complete the steps are described in the following pages.





Each of the steps and the utilities and programs required to complete the steps are described in the following pages. Here is a summary of the steps and the sections in which they are described:

1. Account Request and Approval (Steps 1-3) – Section 4.1
2. Account Request File Processing (Steps 4-7) – Section 4.2
3. On-Line Certificate Request (Step 8) – Section 4.3
4. System User Certificate Approval (Steps 9-12) – Section 4.4
5. System User Certificate Verification (Steps 13-14) Section 4.5
6. System User Certificate Retrieval (Steps 15-16) – Section 4.6

4.1 Account Request and Approval (Steps 1-3)

See section 3.3 for Account Request and Approval information.

citi

4.2 Account Request File Processing (Steps 4-7)

4.2.1 Overview

The Arterium Security Administrator is not responsible for approving access requests to Arterium. This responsibility lies with the Business Manager. Once the Arterium Security Administrator receives the signed and encrypted ARF from the Business Manager, this means the requests have been approved and are ready for processing. The Arterium Security Administrator should review and log the account requests, and then send the reviewed file to the LDAP Operator for import into the Arterium LDAP directory.

The ARF is an abbreviated form of an LDIF file. The ARF must be converted to a full LDIF file before it can be imported into the LDAP system, to create accounts for pre-authorized users. The LDIF File Generator utility is used to create the full LDIF file.

The LDIF file created by the LDIF File Generator utility must be imported into the LDAP to create the accounts for pre-authorized users.

4.2.2 Step-by-Step Process

1. Follow Steps 1-12 in Section 3.4.2
2. Separate out the system user accounts from the Account Request file. These are those with the roles activCardServer and badgingStation. Save this as a separate file. This file is now called the System Account List.
3. Send the System Account List to the RA Administrator via signed and encrypted e-mail.

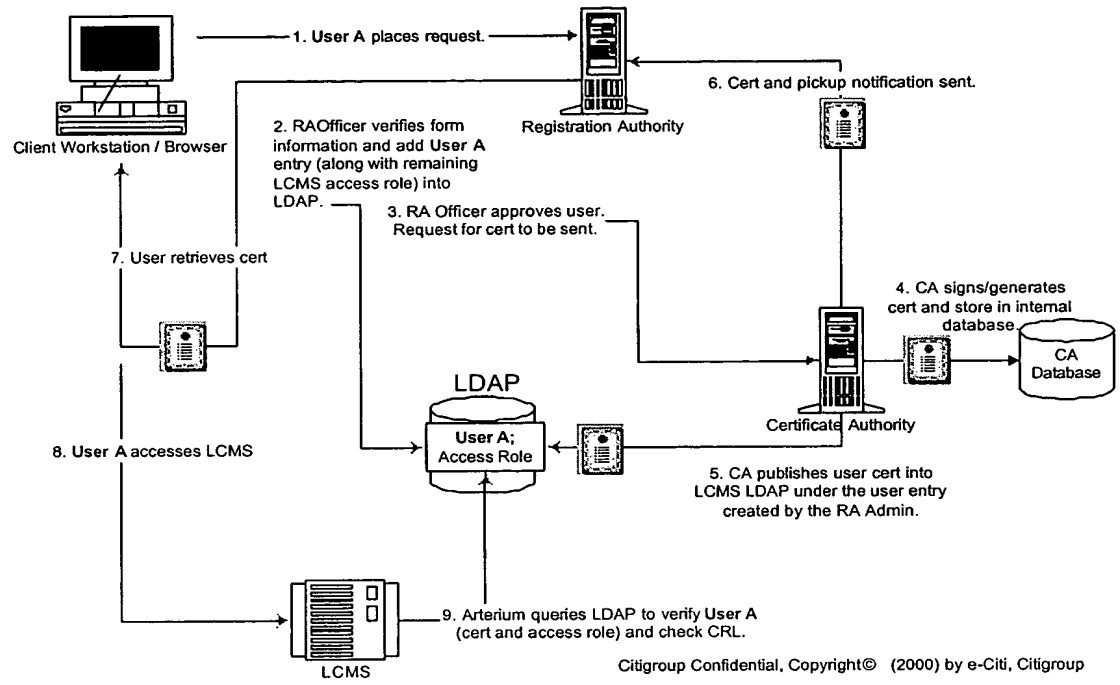
4.3 On-Line Certificate Request (Step 8)

4.3.1 Overview

A system user certificate is necessary to communicate with Arterium. For example, a badging station would require a system user certificate. When the badging station prints a Sun Badge, the badge's status changes from 'Blank' to 'Printed'. Thus, the badging station needs a server user certificate in order to communicate this change to Arterium. The System User Administrator completes the process to request and download a "System User" certificate from Arterium

4.3.2 System Architecture

The following diagram shows the process for the request, approval and retrieval of a System User Certificate.



4.3.3 Step-by-Step Process

NOTE: Before starting this process, make sure the JDK and JSSE are installed on the target system, and the security file is properly setup. See section 4.3.4 for instructions.

1. System User Administrator creates a keystore (or another form of file-based certificate database). This command generates a private/public key pair within the keystore file.

    a. For Java-based keytool keystores, the command is as follows:

    ```
    keytool -genkey -v -alias clientkey -keyalg RSA -sigalg
    SHA1WithRSA -keystore <name and location of keystore file>
    ```

    b. You will be prompted for the following information:

    ```
    Enter keystore password: <password for keystore file>

    What is your first and last name?
      [Unknown]: <enter the FQDN of the server name>(i.e.
    badgingstation.sun.com).
    ```

    NOTE: The 'CN' (for first and last name) must be equal to the FQDN of the server that is to connect to the LCMS. This server name also needs to equal the name submitted with the account request file.

    ```
    What is the name of your organizational unit?
      [Unknown]:  <leave blank>

    What is the name of your organization?
      [Unknown]:  <must enter 'Citibank'>
    ```

```
What is the name of your City or Locality?
  [Unknown]:  <name of City> (i.e. Menlo Park)

What is the name of your State or Province?
  [Unknown]:  <state abbreviation> (i.e. CA)

What is the two-letter country code for this unit?
  [Unknown]:  US

Is <CN=badgingstation.sun.com, OU=blank, O=Citibank, L=Menlo Park,
ST=CA, C=US> correct?
  [no]:  <enter 'y' if correct>

Generating 1024 bit RSA key pair and self-signed certificate
(SHA1WithRSA)
        for: CN=badgingstation.sun.com, OU=blank, O=Citibank, L=Menlo
Park, ST=CA, C=US

Enter key password for clientkey
        (RETURN if same as keystore password): <press RETURN>
```

2. Once the public/private key pair has been created, the next step is to generate a server certificate request (so that the certificate can be signed by a recognized Root CA).

   a. For Java-based keytool keystores, the command is as follows:

      keytool -certreq -v -alias clientkey -file *<name and location of file containing certificate REQUEST>* -keystore *<name and location of keystore>*

   b. The following will be displayed:

      Enter keystore password: <enter keystore password>
      Certification request stored in file *<name and location of file containing certificate REQUEST>*

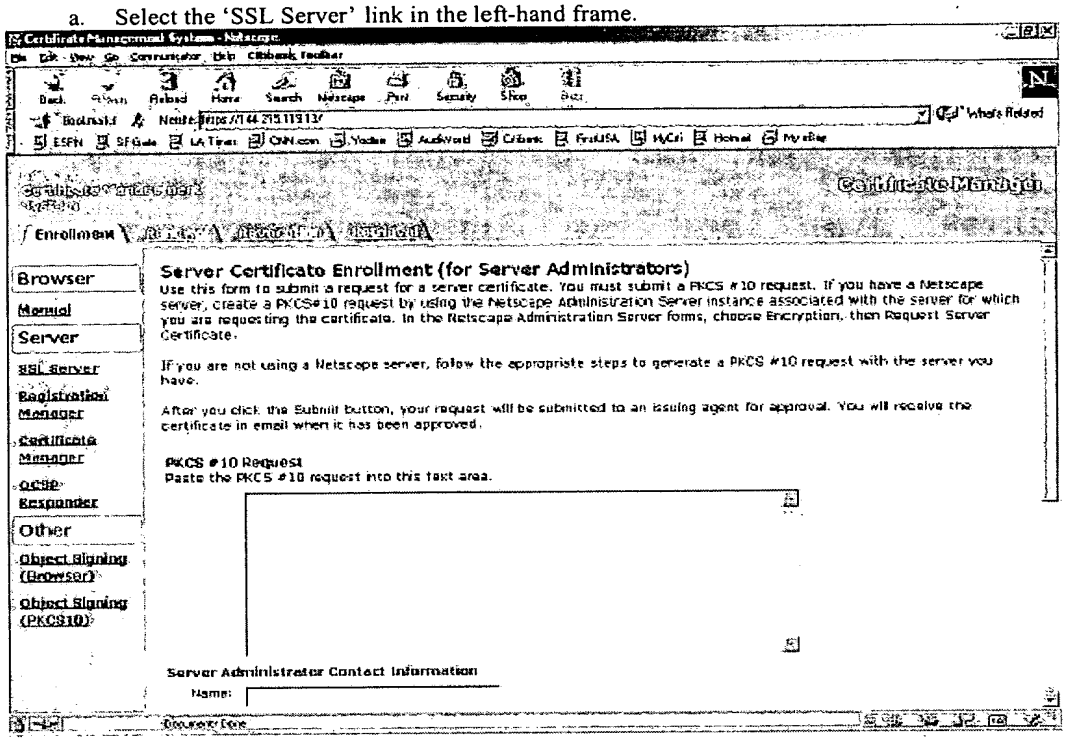
   c. Below is a sample of the contents of the certificate request file:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBqzCCARQCAQAwazELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAkNBMRQwEgYDVQQHEwtMb3MgQW5n
ZWxlczEOMAwGA1UEChMFQ0RDTEExETAPBgNVBAsTCENpdGliYW5rMRYwFAYDVQQDEw1HYW5lc2gg
UHJhYmh1MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDanKVY/Jt11a89ATNia0JXZluNsaHo
Zs6mIW+FbIx34crw9zlZ4V4l3SD6b7V7u4UUJswyP6N1m1N18XEmb3SUMpNojgeHGCOrsjsXTJ/1
PZU7Lqh2szsVlWOC3YMsPBJGh3HFfvEJnP961k30dcgCeECja2Q1EXGCUWunHv1itwIDAQABoAAw
DQYJKoZIhvcNAQEEBQADgYEA2TekR1A5fp6TjnDQ2e/UNwIWwJroOR/ovprgwGLq3h3A3G+3ViZJ
AzGrPxsLaq91j0k+i5gpI6novWIthAce6Y31LorKiM0hTAxnonc21NtvBCvm8066P+DE9qRQP2al
fHwOau/hJ2gQmUjwCluGhaBcFehB/0zBn1tuK1IApx8=
-----END NEW CERTIFICATE REQUEST-----
```

3. Copy the contents of this file (including the `-----BEGIN NEW CERTIFICATE REQUEST-----` and `----END NEW CERTIFICATE REQUEST-----` lines) to the clipboard.

4. Launch the Netscape browser and access the Citibank Smart Access RA Certificate Enrollment form located at: https://www.cardmanagement.citibank.com:8144.

a. Select the 'SSL Server' link in the left-hand frame.



b. **Paste** the copied server certificate request into the text area under "PKCS #10 Request".

c. Enter in the Server Administrator contact information (Full name and email address). These pieces of information need to be as they appear in the Account Request File.

d. Click 'Submit'.

e. Record the Request ID number that is returned. You will need this number when retrieving the approved certificate.

5. Ensure that the Program Administrator has sent an Account Request File for the new System User connection.

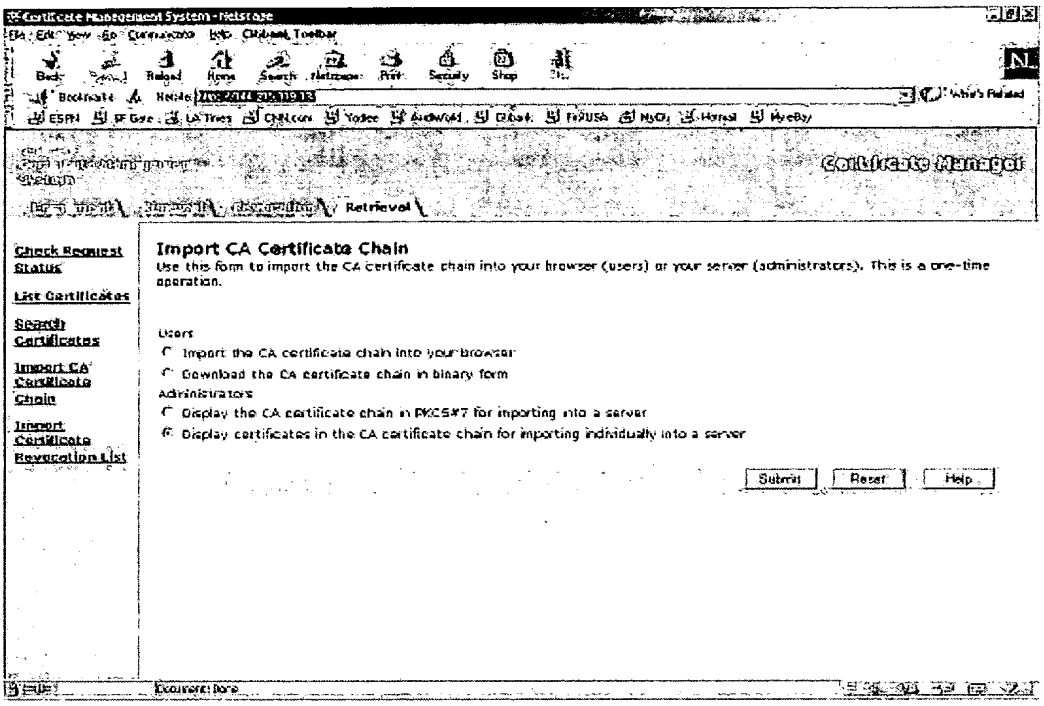
6. In the mean time, while waiting for the certificate approval, the System User Administrator should import the Citibank Root CA certificate chain into the keystore file (or other file-based certificate database).

   a. Return to the RA page.

   b. Click on the 'Retrieval' tab.

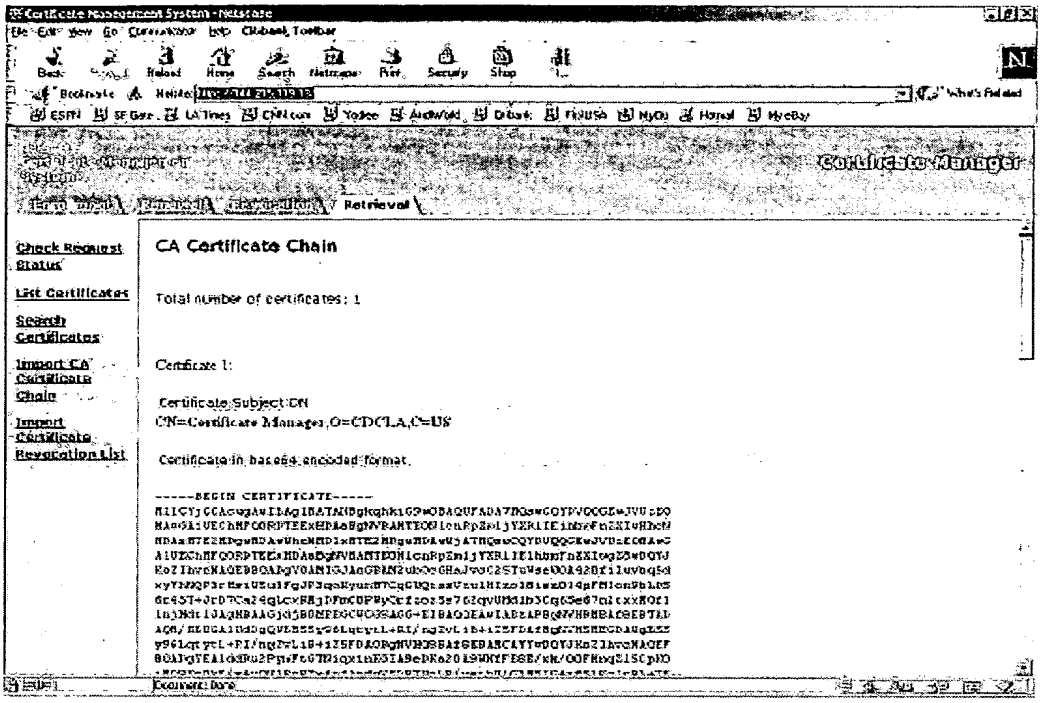
   c. Click on the 'Import CA Certificate Chain' link.

   d. Select the option 'Display certificates in the CA certificate chain for importing individually into a server' and click 'Submit'.



e. A page containing the CA Certificate Chain will be displayed. Copy the entire *base64 encoded* CA Certificate chain (including the `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` lines) and paste it into a text file on the server.

NOTE: the java utility 'keytool' is very picky with the text files it processes. It is recommended that, when using a Windows/MSDOS-based PC platform, that the certificate be pasted into a text editor that supports UNIX-style encoding (i.e. removes the carriage return character '^M' from the file). An example of such a text editor is TextPad (available from http://www.textpad.com).



f. Import the CA certificate chain into the keystore (or file-based certificate DB) using the respective utilities/commands. For Java-based keytool keystores, the command is as follows:

```
keytool -import -v -alias citibankca -file <name/location of
text file containing CA cert> -keystore <name/location of
keystore file>
```

i. Enter the password when prompted.

ii. A screen *similar* to the following will be displayed:

```
Owner: CN=Certificate Manager, OU=Citibank, O=CDCLA, L=LA,
ST=California, C=US
Issuer: CN=Certificate Manager, OU=Citibank, O=CDCLA, L=LA,
ST=California,C=US
Serial number: 1
Valid from: Mon Oct 16 00:00:00 PDT 2000 until: Wed Oct 16 00:00:00
PDT 2002
Certificate fingerprints:
MD5:  EE:DA:64:BA:81:3D:64:E6:5B:17:6D:19:69:97:0A:48
SHA1: 68:F6:83:2B:64:A0:44:14:9B:DD:A6:69:5D:EC:F0:AE:AC:BF:77:F2

Trust this certificate? [no]:
```

iii. Type '`yes`' to trust the certificate and add it to the keystore file. If successful, the following message will be displayed.

```
Certificate was added to keystore
```

NOTE: To view the keystore file, type the following command:

```
keystore -list -v -keystore <yourfilename>
```

4.3.4 System Requirements

Before the system user certificate request and issuing process can progress, the following must be accomplished on the remote system.

1. Install JDK 1.3 and JSSE on requesting server. (Software can be downloaded from java.sun.com)
2. After installing JSSE, copy the three files (jcert.jar, jnet.jar, jsse.jar) from the jsse1.0.2\lib directory into the c:\jdk1.3\jre\lib\ext folder.
3. Open the java.security file (found in c:\jdk1.3\jre\lib\security directory). Insert the following two lines into the file:

   ```
   security.provider.1=sun.security.provider.Sun.
   security.provider.2=com.sun.net.ssl.internal.ssl.Provider
   ```

4. Save java.security file.
5. Install Text Pad 4 (latest available version) on requesting server. Other text editors tend to add unnecessary carriage returns to certificates. (Software can be downloaded from Textpad.com)
6. The system variables on the requesting machine must be edited. Perform the following steps:
   a. Go to requesting server's Control Panel (from Start Menu).
   b. Click on 'System'. A 'System Properties' window will appear.
   c. Click on the 'Advanced' tab. Next, click on the 'Environment Variables' button.
   d. Find 'Path' under the 'System Variables' list box. Select 'Path' and then click the 'Edit' button, which is displayed below the 'System Variables' list box.
   e. An 'Edit System Variable' window should now be displayed. Append the following line to the end of the items listed in the 'Variable Value' text box: c:\jdk1.3\bin. Next, click 'OK' and exit all Control Panel windows.

4.4 System User Certificate Approval (Step 9-12)

4.4.1 Overview

The RA Administrator will receive the System Account List from the LDAP Operator. For new the system user requests accounts, the information in this list should be compared against the certificate requests that come in from the remote system administrators. If the data matches, the request should be approved.

Look for the following data to match:

- Server name (listed as Common Name (CN)) provided in the certificate request
- Contact info of Requestor (Name, email, phone number)

After the certificate request has been approved, the certificates for the system user will be published to the LDAP database automatically. The Activated System Account List should be sent to the Arterium Security Administrator for verification.

citi

4.4.2 Step-by-Step Process

1. Receive the System Account List via secure e-mail from the LDAP operator.
2. Login to the Approver's RA Site (https://www.cardmanagement.citibank.com:8100/arterium).
3. Search for a specific certificate request or leave the search field blank and view all requests pending approval
4. Once the desired request is located, he clicks on the 'Details' link
5. Compare the certificate information to the System Account List to make sure the following information matches:
   - Server name (listed as Common Name (CN)) provided in the certificate request
   - Contact info of Requestor (Name, email, phone number)information to the on-line certificate requests which are posted to the RA server
6. Make sure this system user exists in LDAP and the Common Name is equal to the FQDN entered in the request (i.e. badgingstation.sun.com)
7. Choose whether to accept, reject, or cancel the request. If he approves it, the certificate is generated and automatically published to the LDAP directory.
8. Send the System Account List, now called the Activated System Account List, to the Arterium Security Administrator via signed and encrypted e-mail and state in the body of the e-mail which requests were accepted or rejected.

4.5 System User Certificate Verification (Steps 13-14)

4.5.1 Overview

The Arterium Security Administrator needs to play the "checker" role of the system user account generation process. The Arterium Security Administrator should verify the correct accounts were created and then notify the requesting organization Program Administrator that the requested certificates are ready for download.

4.5.2 Step-by-Step Process

1. The Arterium Security Administrator receives the Activated System Account List via secure e-mail from the RA Administrator
2. Use the Agent Services of the Netscape CMS to list the certificates created by date. Verify the proper number of certificates were created. Please see the "Agent Services" page for the "Certificate Manager" in the "Netscape CMS Administrator's Guide" for instructions on how to list certificates by date
3. Notify the requesting organization Program Administrator that the requested certificate is available for download. This can be done by sending them the Activated System User Account list, or by a simple e-mail notification.

citi

4.6 System User Certificate Retrieval (Steps 15-16)

4.6.1 Overview

The Program Administrator should notify the System User Administrator that the requested certificate is available for download. The System User Administrator should perform the download of the certificate to the system.

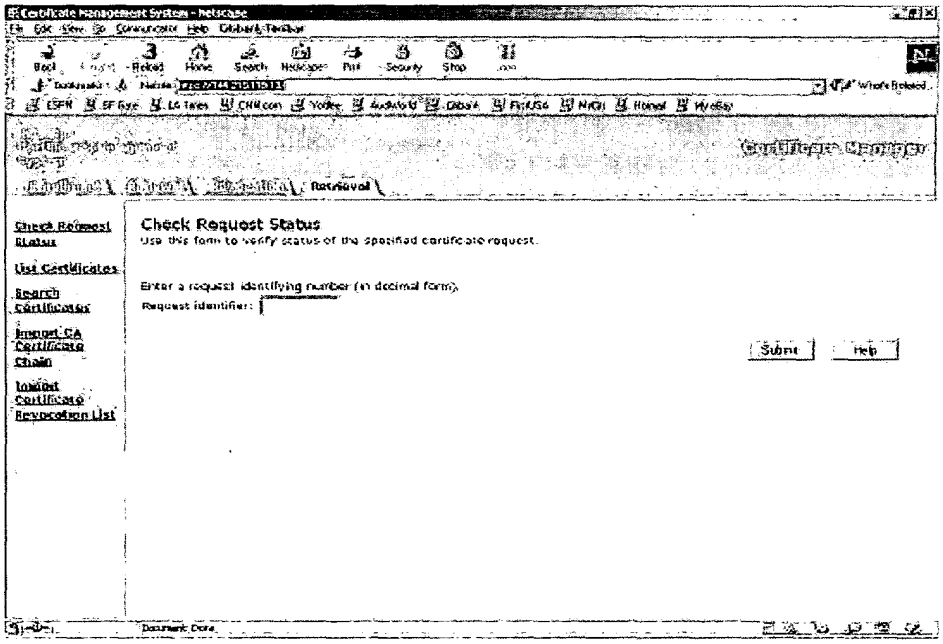
4.6.2 Step-by-Step Overview

1. The Program Administrator receives notification from the Arterium Security Administrator that the requested certificate is available for download
2. The Program Administrator notifies the System User Administrator to retrieve the certificate.
3. System User Administrator then returns to the RA website to retrieve the certificate.

   https://www.cardmanagement.citibank.com:8144.

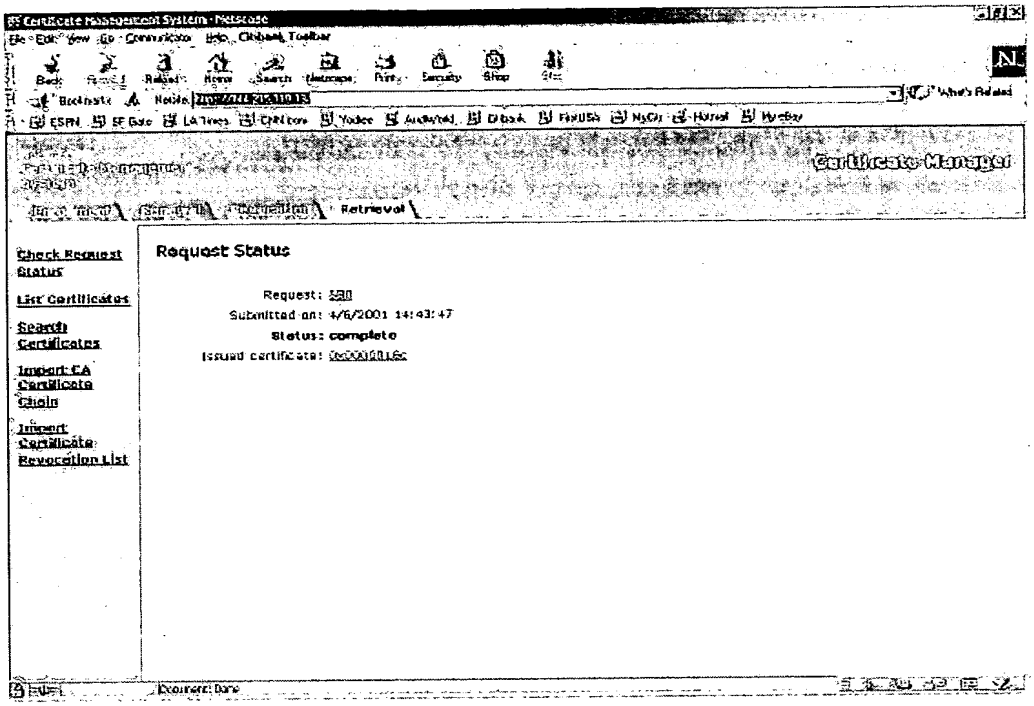
   a. Click on the 'Retrieval' Tab.

   b. Enter the Request ID and click 'Submit'.

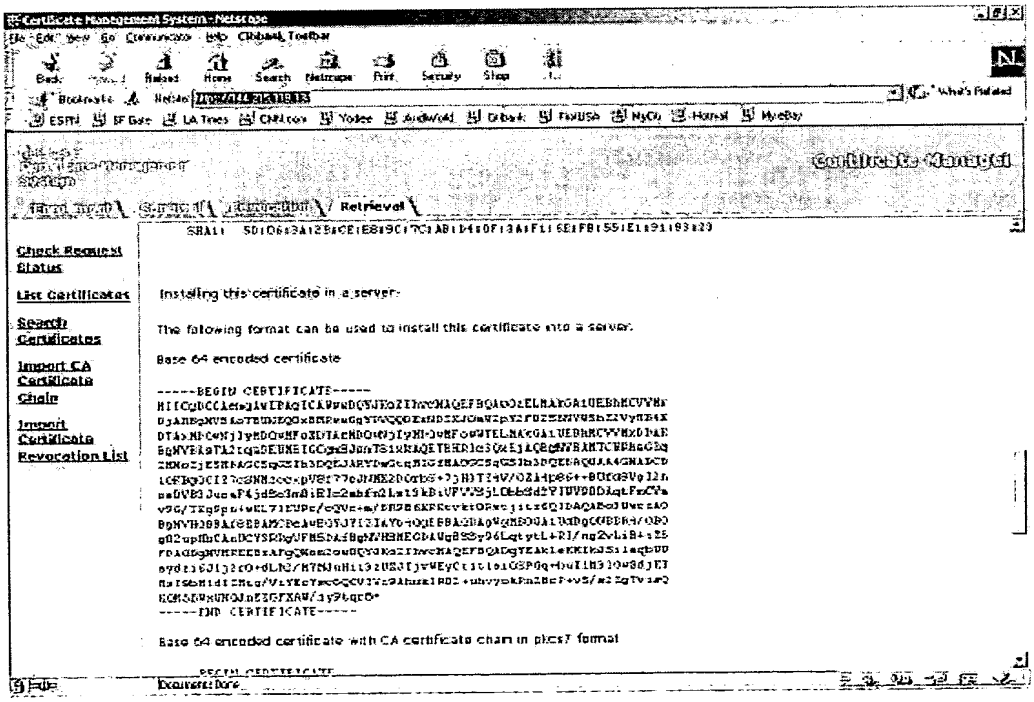


   c. The certificate listing will appear. Click on the 'Issued certificate' serial number to display the actual certificate.

citi



d. Scroll down to the *Base 64 encoded* certificate.



e. Copy the entire certificate (including the `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` lines) and PASTE it into a text file on the server.

NOTE: the java utility 'keytool' is very picky with the text files it processes. It is recommended that, when using a Windows/MSDOS-based PC platform, that the certificate be pasted into a text editor that supports UNIX-style encoding (i.e. removes the carriage return character '^M' from the file). An example of such a text editor is TextPad (available from http://www.textpad.com).

2. Import the server certificate (signed by the Citibank Root CA) into the keystore (or file-based certificate DB) using the respective utilities/commands. For Java-based keytool keystores, the command is as follows:

```
keytool -import -v -alias clientkey -file <name/location of text
file containing signed server cert> -keystore <name/location of
keystore file>
```

   i. Enter the password when prompted. You will need to save this password for future use for certificate renewal.

   ii. If the import is successful, the following will be displayed:

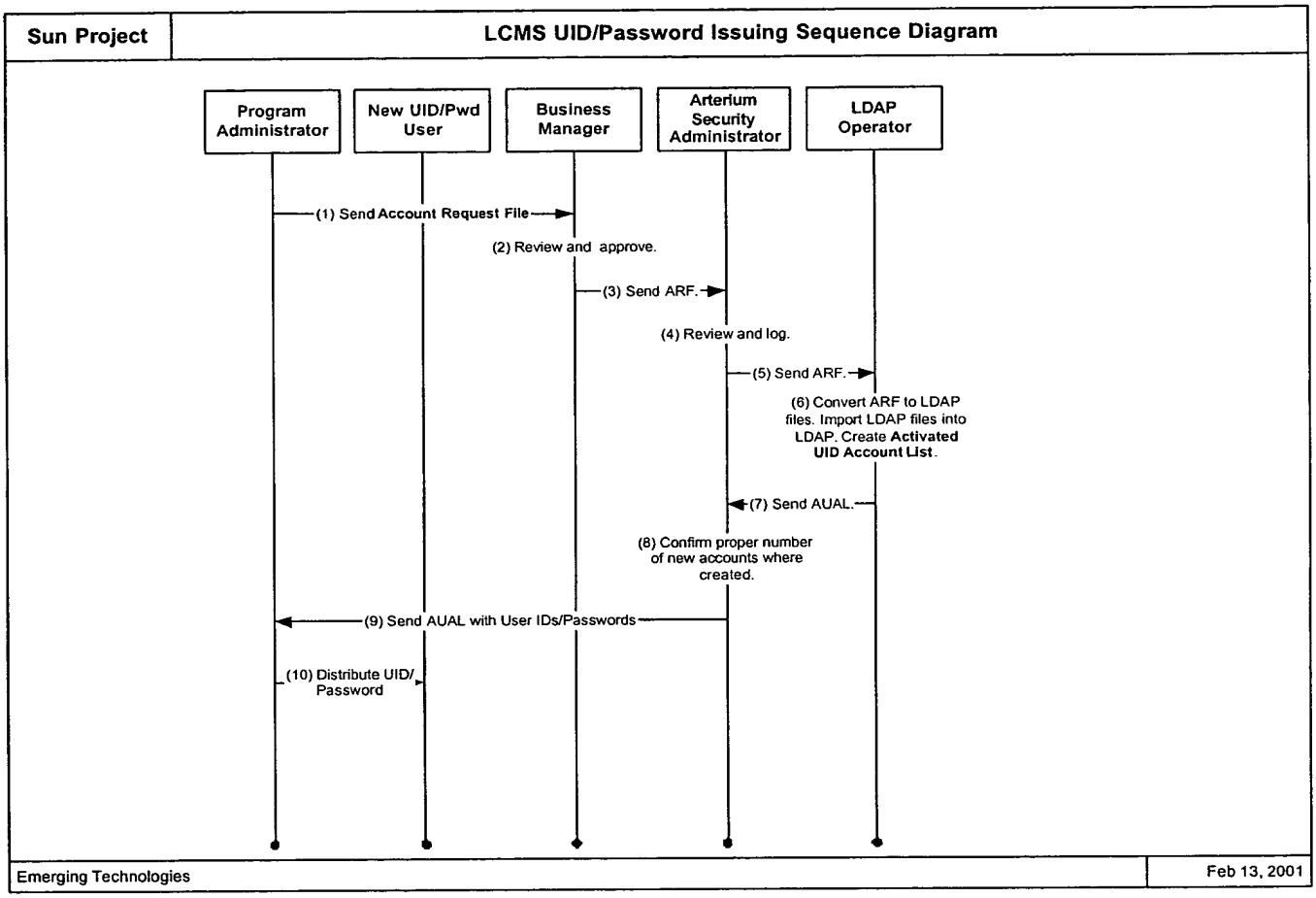
```
Certificate reply was installed in keystore
[Saving <name/location of keystore file>]
```

3. Now that the private key has been generated, the signed public key (certificate) and Root CA certificate have been imported, the keystore is now ready for use with the LCMS XML messaging interface.

citi

5 LCMS UID/Password Issuing Process

The following diagram shows the overall process for LCMS UID/Password Issuance.



Each of the steps and the utilities and programs required to complete the steps are described in the following pages. Here is a summary of the steps and the sections in which they are described:

1. Account Request and Approval (Steps 1-3) – Section 5.1
2. Account Request File Processing (Steps 4-7) – Section 5.2
3. UID/Password Account Verification (Steps 8-9)- Section 5.3
4. UID/Password Account Distribution (Step 10)– Section 5.4

5.1 Account Request and Approval (Steps 1-3)

See section 3.3 for Account Request and Approval information.

citi

5.2 Account Request File Processing (Steps 4-7)

5.2.1 Overview

The Arterium Security Administrator is not responsible for approving access requests to Arterium. This responsibility lies with the Business Manager. Once the Arterium Security Administrator receives the signed and encrypted ARF from the Business Manager, this means the requests have been approved and are ready for processing. The Arterium Security Administrator should review and log the account requests, and then send the reviewed file to the LDAP Operator for import into the Arterium LDAP directory.

The ARF is an abbreviated form of an LDIF file. The ARF must be converted to a full LDIF file before it can be imported into the LDAP system, to create accounts for pre-authorized users. The LDIF File Generator utility is used to create the full LDIF file.

The LDIF file created by the LDIF File Generator utility must be imported into the LDAP to create the accounts for pre-authorized users.

5.2.2 Step-by-Step Process

1. Follow Steps 1-12 in Section 3.4.2

2. Separate out the UID/password user accounts from the Account Request file. These are those with the roles sunHelpDeskOfficer and HostingAdminOfficer. Save this as a separate file. This file is now called the Activated UID Account List.

3. Send the Activated UID Account List to the Arterium Security Administrator via signed and encrypted e-mail.

5.3 UID/Password Account Verification (Steps 8-9)

5.3.1 Overview

The Arterium Security Administrator needs to play the "checker" role in the UID/password account creation process. The Arterium Security Administrator should verify the correct accounts were created and then send the new account information to the requesting organization Program Administrator.

5.3.2 Step-by-Step Process

1. The Arterium Security Administrator receives the Activated UID Account List from the LDAP operator via signed and encrypted e-mail.

2. Verify the correct accounts were created

3. Send the Activated UID Account List to the requesting organization Program Administrator via signed and encrypted e-mail.

5.4 UID/Password Account Distribution (Step 10)

The Program Administrator is responsible for securely distributing the new UID/password information to the correct end users. The Program Administrator should securely archive the Activated UID Account List for future reference.

6 Certificate Re-Issuance Process

6.1 Overview

The client certificates issued for LCMS Admin Cards and System Users will periodically expire. When the certificates expire, a new certificate must be generated and download to the LCMS Admin Card or the remote System. The process below describes this certificate re-issuance process.

6.2 Certificate Check Cron Job

This is a design for how the certificate check cron job would operate. The actual script to run and the cron job would need to be developed.

> Once daily, the *cron* job on the RA will start up a PERL script (`CertCheck.pl`) to notify end users that their certificates are soon to expire. The users will be targeted by their role.
>
> The LDAP directory will be referenced for each user with a given role. The certificate will be accessed and the expiration date will be gleaned from the certificate. The user's name (cn) will be accessed from the LDAP entry as will the email address (mail). If these attributes do not exist in the LDAP, then they will be gleaned from the certificate.
>
> The current GMT (Greenwich Mean Time) will be compared to the expiration time of the certificate. One week prior to certificate expiration, the script shall start sending emails to the certificate owners advising them that their certificates are soon to expire and will direct them to the RA web page for automatic renewal.
>
> Multiple versions of the PERL script can be run by multiple entries in the *crontab*, each targeting a different role. Modifying the entry in the crontab can change the granularity of the notification.

6.3 User Notification

When the user's certificate is soon to expire, they will receive an email to remind them to renew their certificate. They will receive an email once a day until they complete the renewal process.

The email may have a similar message as follows:

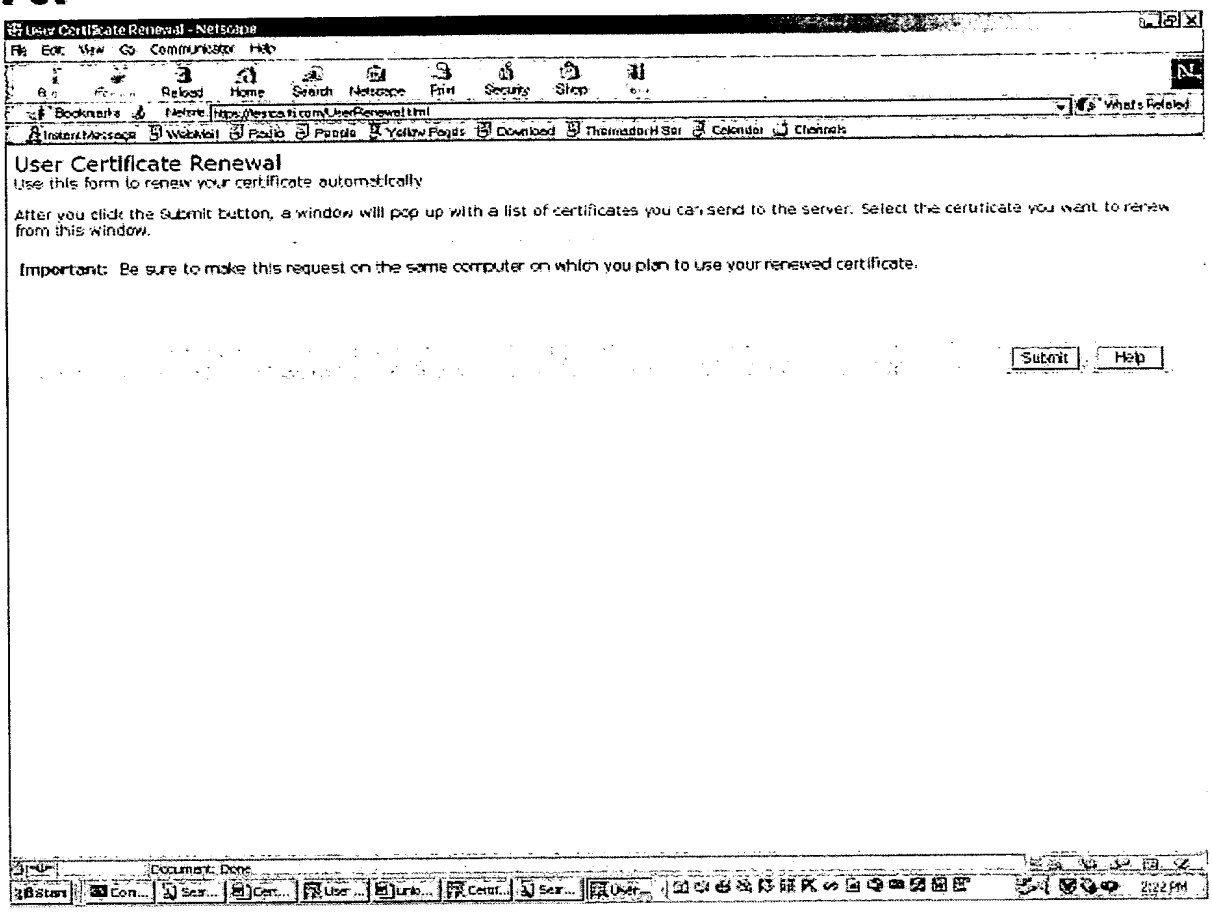
```
Dear Elvis Schmendekamp,
Your Certificate is to expire on August 24, 2001.  Please renew your certificate by
visiting https://testca.tti.com/UserRenewal.html
Thank you.
```

The user then may connect to the web page by clicking on the link name (https://testca.tti.com/UserRenewal.html). It is important to complete this process before the certificate expires so that no loss in LCMS service is experienced.

6.4 Certificate Renewal Process

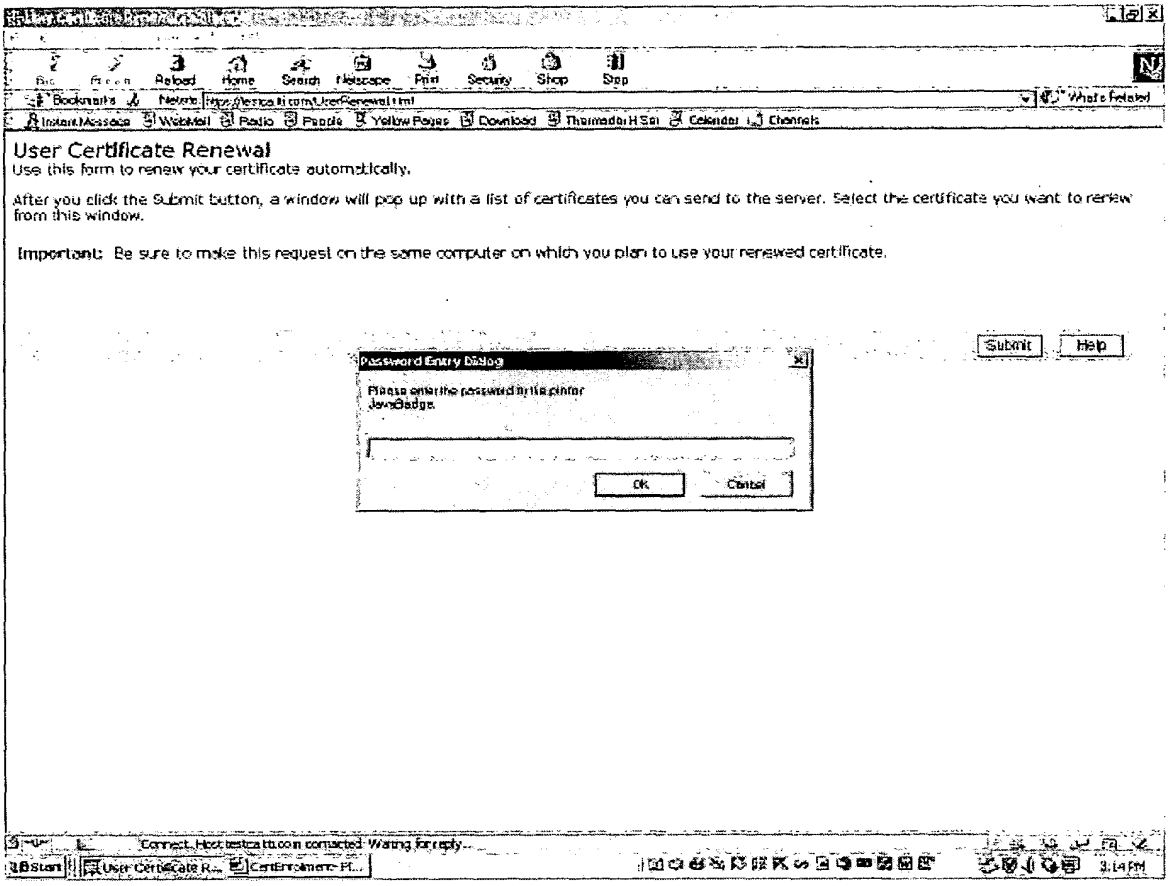
1. The user connects to the web page by clicking on the link name in the received email reminder (https://testca.tti.com/UserRenewal.html) and will be directed to click the "Submit" button.

citi


User Certificate Renewal - Netscape
File Edit View Go Communicator Help
Reload Home Search Netscape Print Security Stop
Bookmarks Netsite: https://esscan.com/UserRenewal.html
What's Related
Instant Message WebMail People Yellow Pages Download Thomasbrill Bar Calendar Channels
User Certificate Renewal
Use this form to renew your certificate automatically
After you click the Submit button, a window will pop up with a list of certificates you can send to the server. Select the certificate you want to renew from this window.
Important: Be sure to make this request on the same computer on which you plan to use your renewed certificate.
Submit
Help
Document: Done
Start
2:22 PM

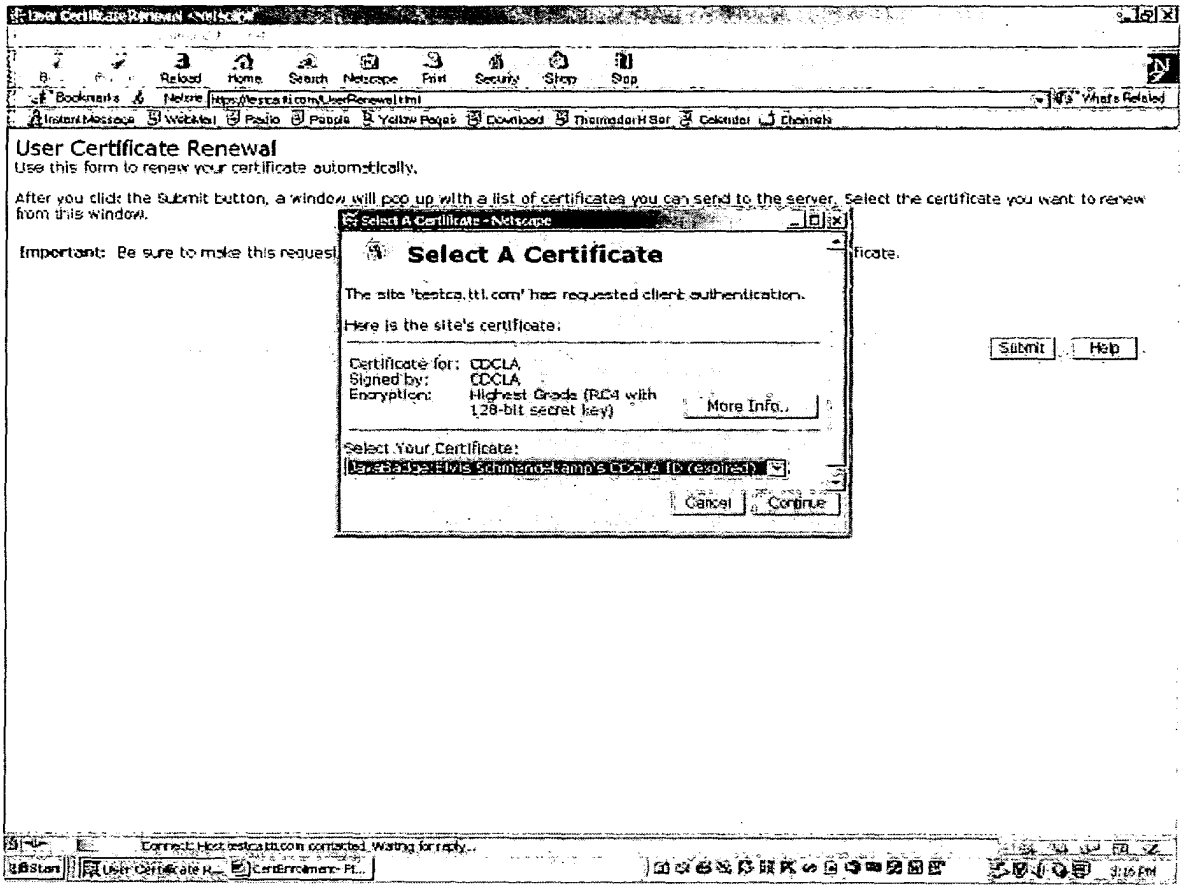
citi

2. The user will be prompted for a password. If the certificate is stored on a smart card, the user should enter their Card PIN. If the certificate is stored in the browser, this is the password to the certificate storage database on the system. The user should enter the PIN/password and click "OK".



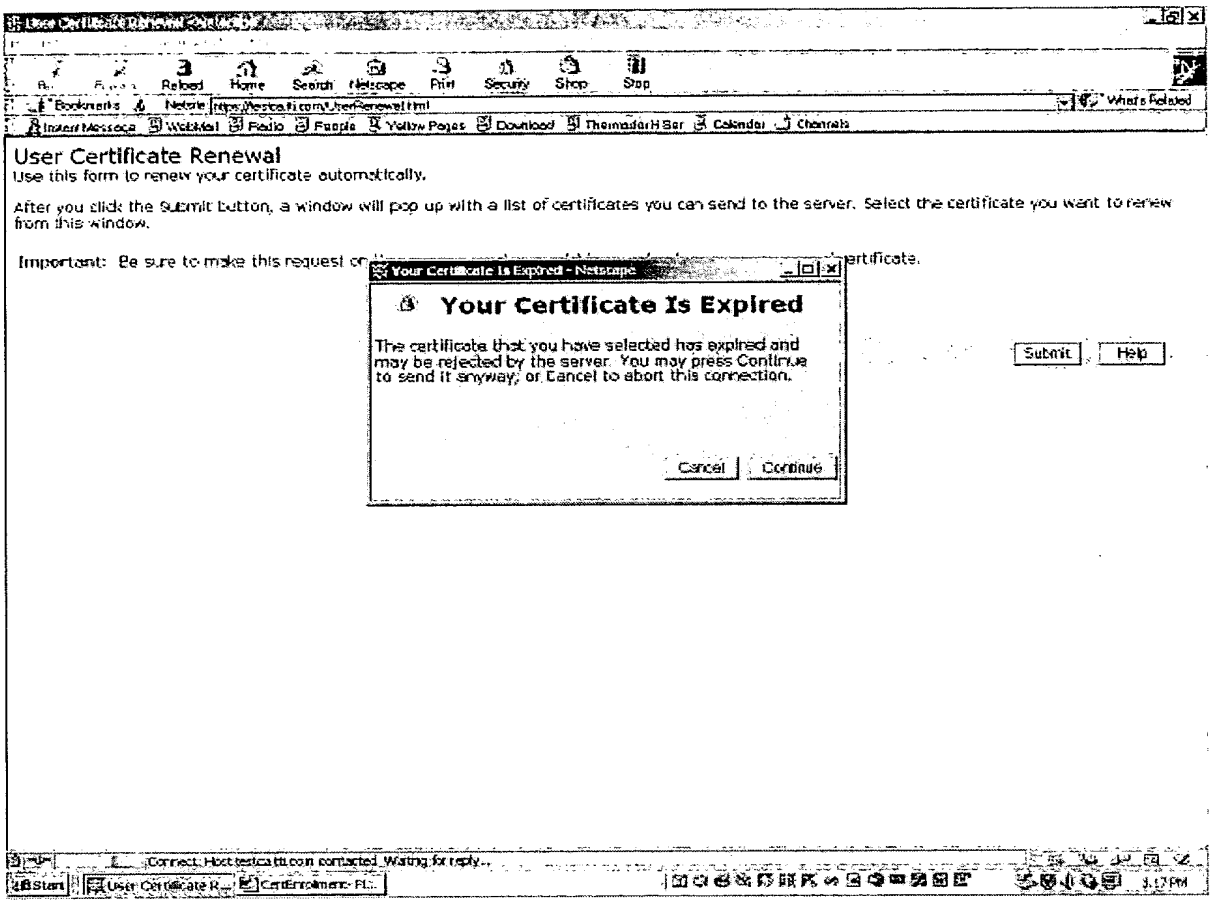
3. The user is then shown a list of certificates that can be renewed by this Certificate Authority.

citi

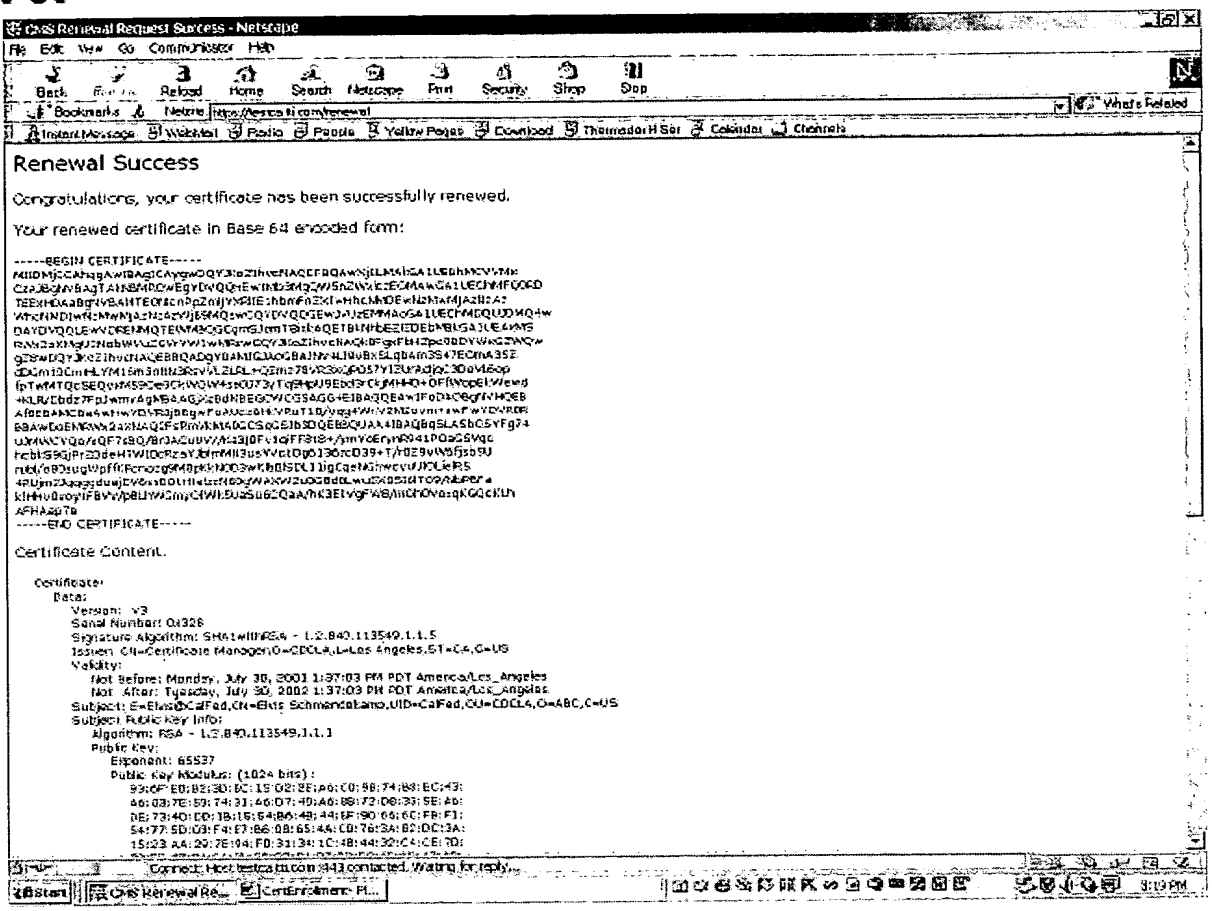


4. The certificate to be renewed should be selected by default. Verify the correct certificate is selected and then click the "Continue" button.

5. The user may be advised that the certificate is expired. If the certificate is still valid, the user will not encounter this screen. The user then clicks the "Continue" button and the certificate request will be processed.



6. After a small delay, the certificate will be processed and the following screen will appear:



7. The updated certificate is now on the smart card or in the browser.

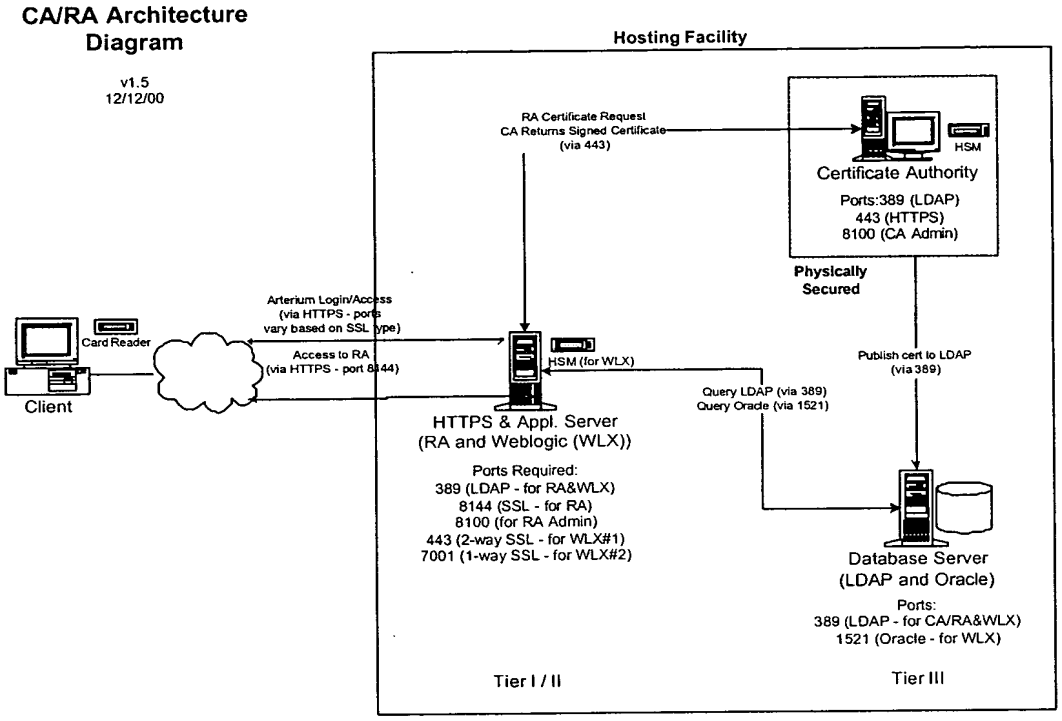
citi

Appendix A: Acronym List

Acronym	Definition
CDL	Card Data List
LDAP	Lightweight Directory Access Protocol
LCMS	Lifecycle Management System
SSL	Secure Sockets Layer
CA/RA	Certificate Authority/Registration Authority
PKI	Public Key Infrastructure
LDIF	Lightweight Directory Input File??
PCL	PIN Creation List
CAL	Certificate Account List
PGP	Pretty Good Privacy
PIN	Personal Identification Number
ACI	Administrator Card Issuing
UID	User ID
HSM	Hardware Security Module
CSR	Customer Service Representative
XML	Extended Markup Language
LDAP	Lightweight Directory Access Protocol
CMS	Certificate Management System
ARF	Account Request File
ACL	Activated Card List
SAL	System Account List
FQDN	Fully Qualified Domain Name

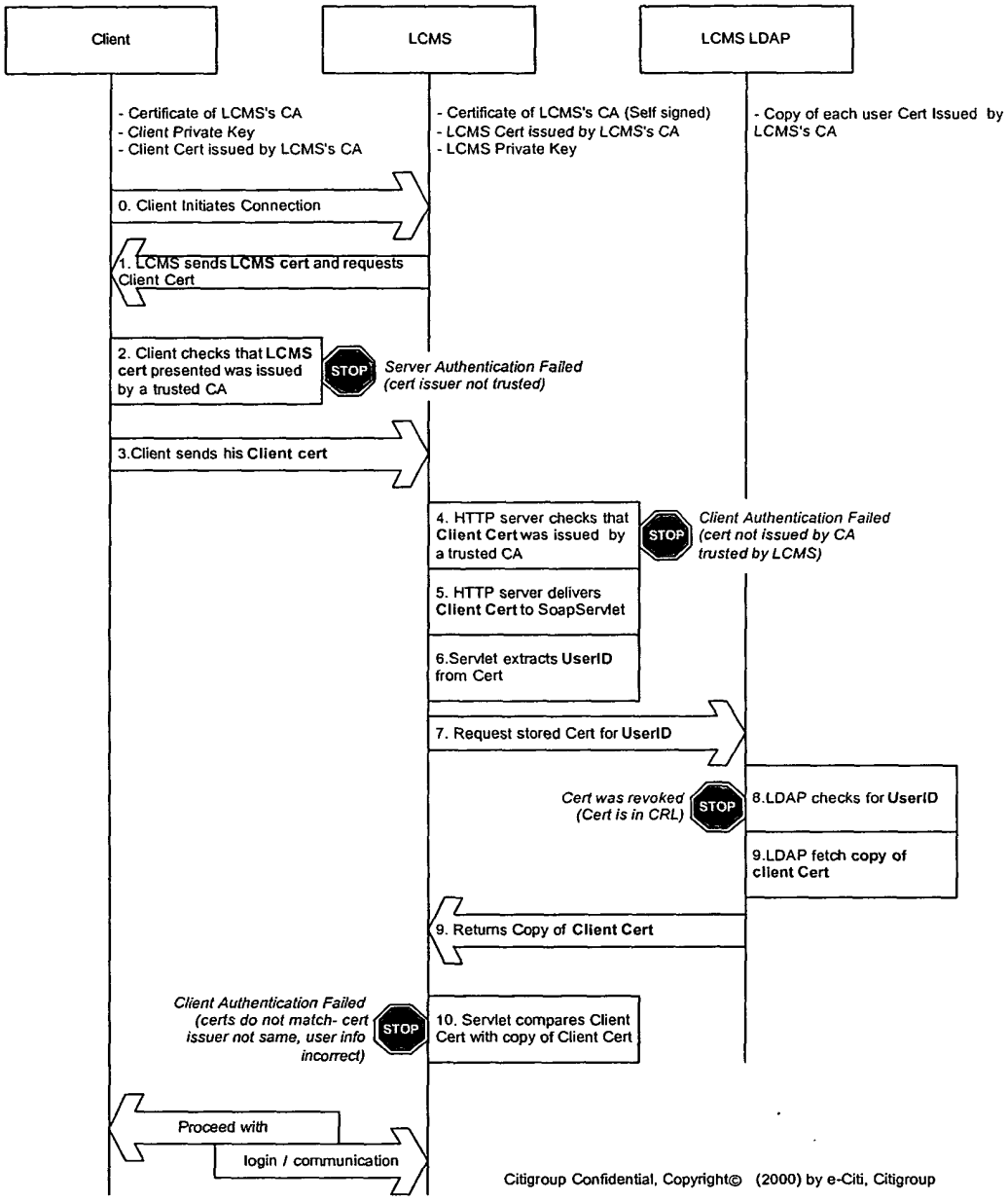
citi

Appendix B: LCMS Network Service Requirements



Appendix C: LCMS Certificate Based Access Control

The following diagram shows the messaging flow for a certificate based authentication to the LCMS.



citi

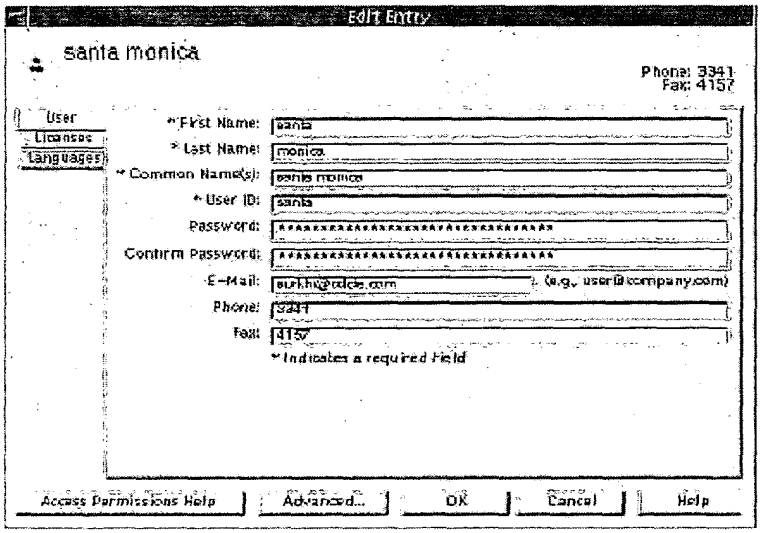
Appendix D: Test Environment LCMS Admin Card Issuance

1. Create a new user in the test LCMS LDAP directory

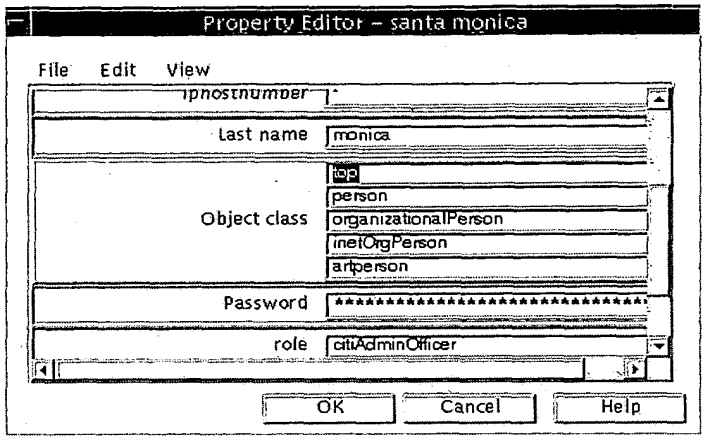
2. Launch the iPlanet Diectory Server console. Click on the 'Directory' tab to access the LDAP user directory.

3. Click on the root folder (i.e. CDCLA) and from the menu bar, select 'Object->New->User'

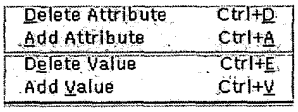
4. The following screen will appear. In the following example, a user by the name of santa monica will be used. Fill out the edit entry screen with the information about the new test user:
   - First Name – First name of intended user
   - Last Name – Last name of intended user
   - Common Name – Organization identifier and last name of user in the format of org-lastname. (i.e. citi-doe)
   - User ID – enter the same as the common name
   - Password – enter "citibank" this password is not used by the user for login
   - E-mail – not required, but enter e-mail address of intended user if it exists



5. Click on the 'Advanced' option to add additional attributes required by Arterium. The following Property Editor screen will appear:

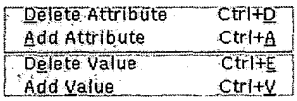


6. Right click on 'Object class' and a menu will pop up with the following 4 options:



7. Click on 'Add Value' and select the "artperson" object class from the menu provided and click 'OK'.

8. Right click on 'Object class' again and now select the 'Add Attribute' option.



9. In the attribute list that appears, scroll down until the entry 'iphostnumber' appears. Select this item and click 'OK'. In the entry field, type in '*' to allow the user access to Arterium from any IP address.

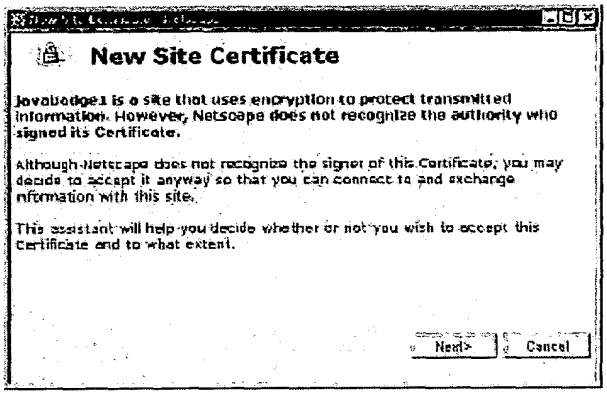
10. Select to 'Add Attribute' again and this time select 'role'. For the role, enter in the designated Arterium role for the current user request. Select either citiAdminOfficer, sunBadgingOfficer or Vendor

11. Repeat the previous step for the 'defaultpartition' entry. Enter in the designated card partition the current user has access to (i.e. 'sun' for access to the Sun card database, and 'citi' for access to the Citibank card database.)

12. Once the iphostnumber, defaultpartition, and role entries have been added and populated, click on 'OK' to complete the creation of the user entry. NOTE- The user information (especially user name and ID) entered into the LDAP database for this user must match EXACTLY the information that is submitted in the certificate request. The CA uses this information to publish user certificates into the correct LDAP entry.

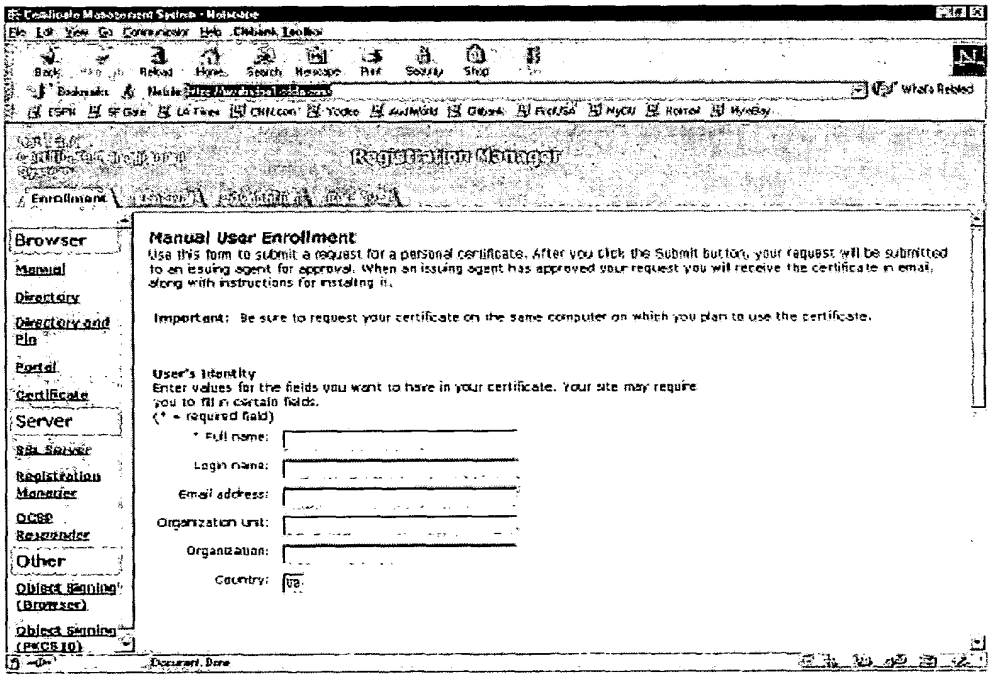
13. Using a PC with ActivCard Gold 2.0 and a reader installed, initialize the new Admin Card according to the Gold instructions. Note the Card PIN and Unlock Code.

14. Connect to the test RA server URL: https://*hostname.of.RA*. If this is the first visit to the website, you will be prompted to accept a site certificate.



15. Follow the instructions and click 'Next' until prompted to click the 'Finish' button.

16. Once the certificate is accepted, the CMS Registration Manager page will appear. Fill out the Manual Enrollment form.

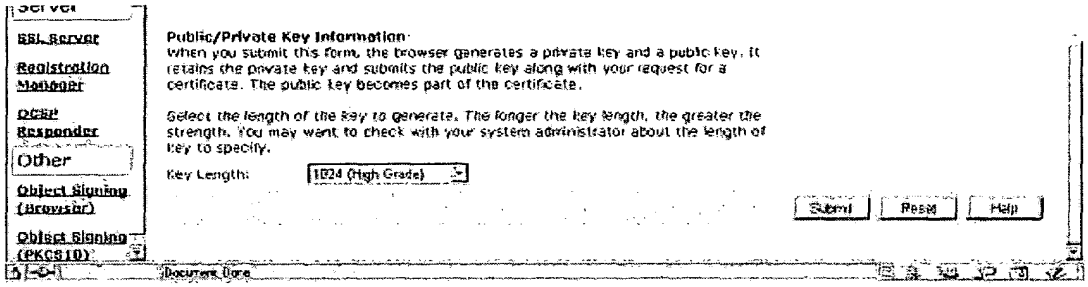


NOTE: The Full Name MUST match the Common Name LDAP directory entry, and the Login Name MUST match the User ID LDAP directory entry.

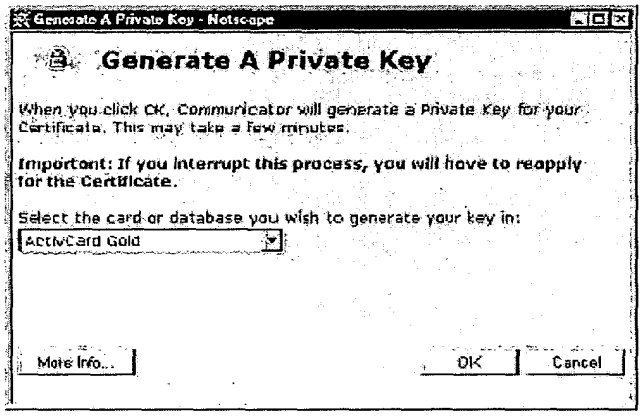
citi

- Full name = Full Name of user of Test LCMS Admin Card
- Login Name = Login ID of user of Test LCMS Admin Card
- Email address = Your E-mail address. This will be used to send you a notification that the certificate is ready for retrieval.
- Organizational Unit= Citibank (should match what is established for LCMS)
- Organization= TBD
- Country = US

17. *Once the form is completed, click on 'Submit' to send the request.*

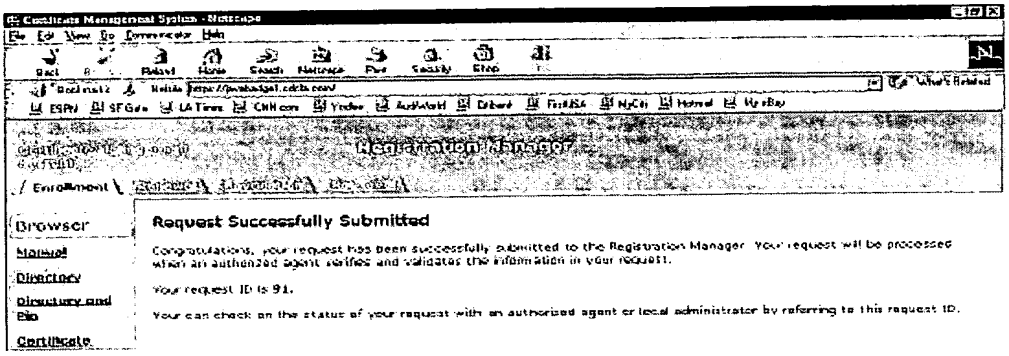


18. At this point, a private/public key pair will be generated. Select where the key pair is to be generated. Select the ActivCard database for keypair generation on the card. This step assumes that the ActivCard software has been installed and is operating properly.



19. Once the key pair has been generated, the certificate (public key) associated with the certificate is sent to the Registration Authority (RA) as a certificate request. A page will appear verifying that the request has been sent and is awaiting approval by the RA Administrator.

citi

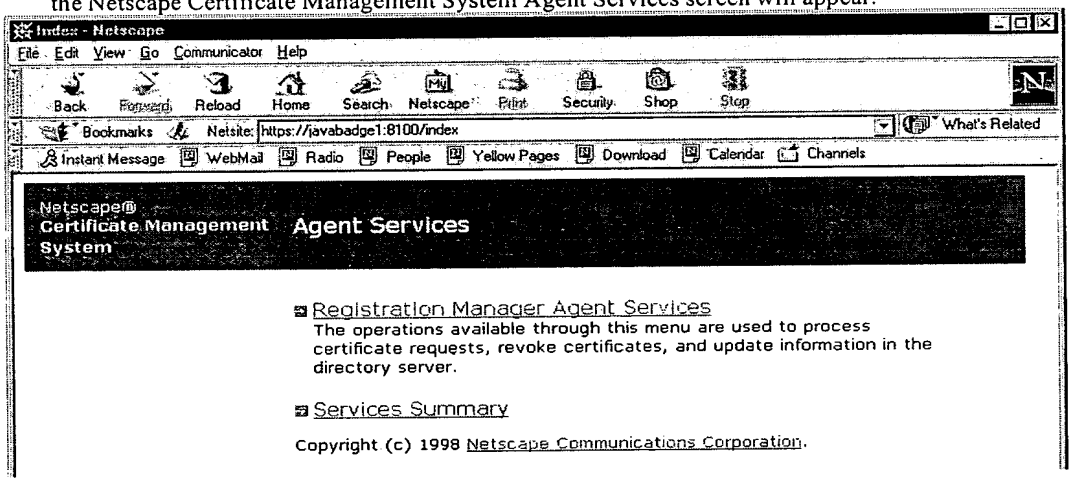


20. As the "RA Administrator" connect to the test RA server. URL: https://*hostname.of.RA*:8100. If this is the first time visiting the site, you may be prompted to accept the site certificate.

21. Follow the instructions and click on 'Next' until you get to the last dialog box with the 'Finish' option.

22. After the site certificate is accepted, Netscape will then send your CMS Agent certificate to the RA. If the user bound to the certificate is not authorized to manage certificate requests (i.e. serve as an authorized agent of the CMS) the user will be denied access to the CMS Agent Services page.

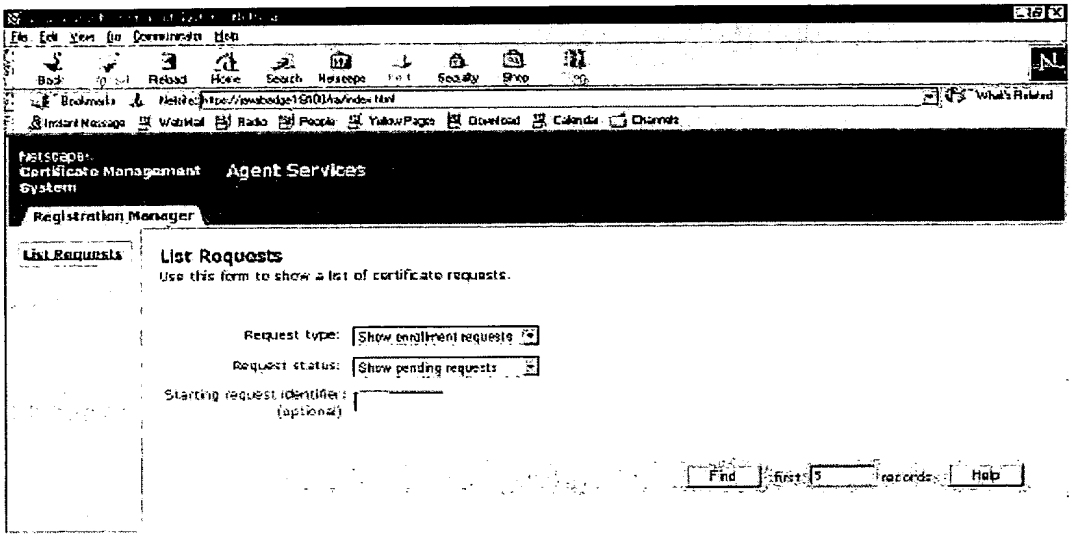
23. Assuming that the user has been issued a valid Agent Certificate, after the site certificate is installed, the Netscape Certificate Management System Agent Services screen will appear.



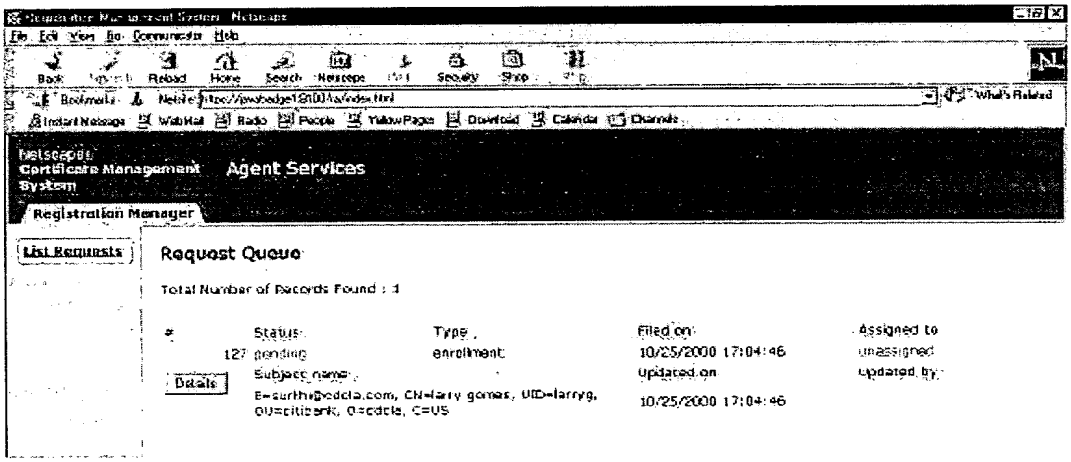
24. Click on 'Registration Manager Agent Services' to access the certificate requests.

25. The 'List Requests' page will appear. From this page, the authorized agent (RA Administrator) can access a single request (using the request identifier issued to the user requesting the certificate) or a set of the most recent requests (by indicating a specific number desired).

citi

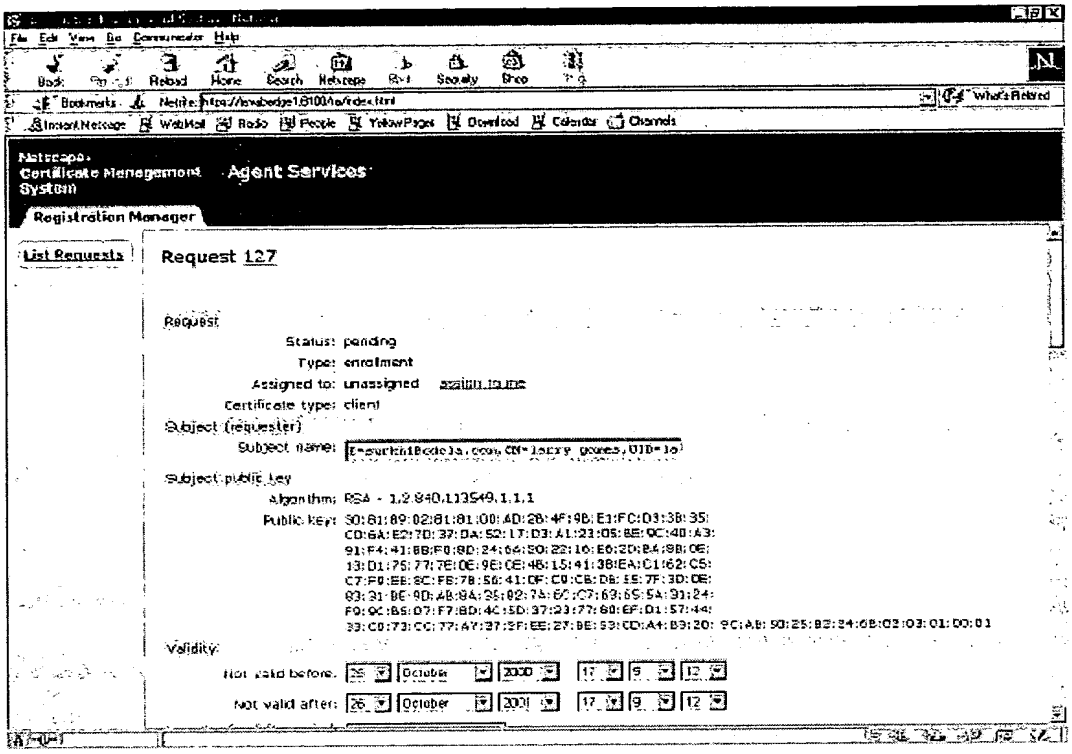


26. In this example, there is only one certificate request that is pending approval. Click on 'Details' to view and manage the certificate request.



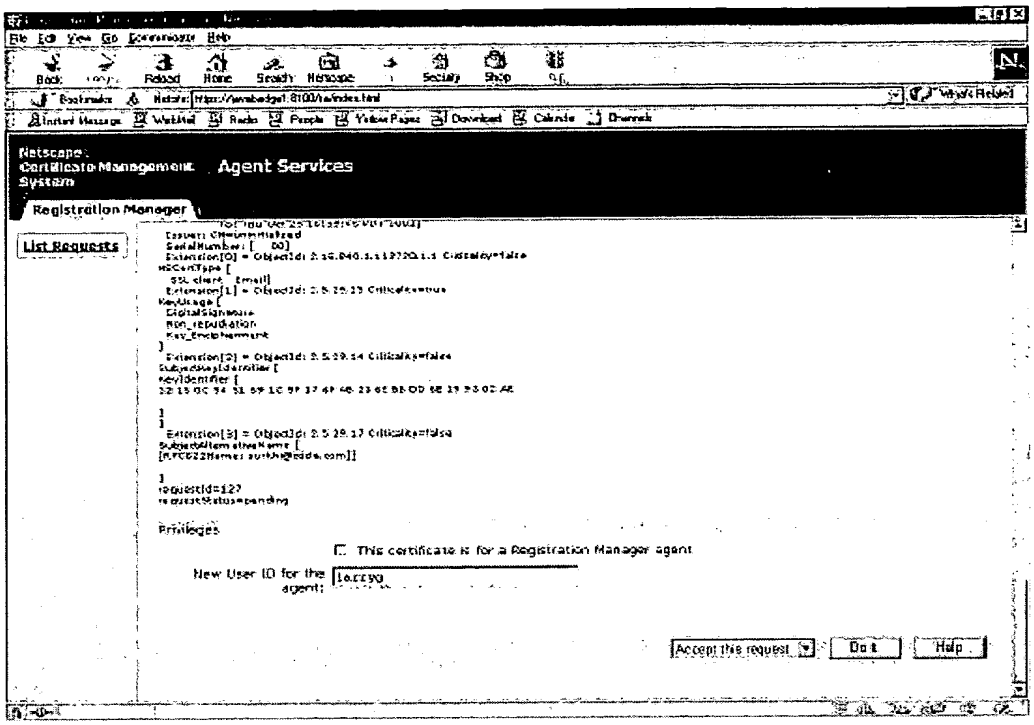
DETAILS SCREEN:

citi



27. If necessary, Click on 'assign to me' to assign the request to yourself. Verify the user information in the request with the information you provided during the enrollment phase.

28. Scroll down to the bottom of the page. Select 'Accept this request' and click on 'Do it' to accept the request.

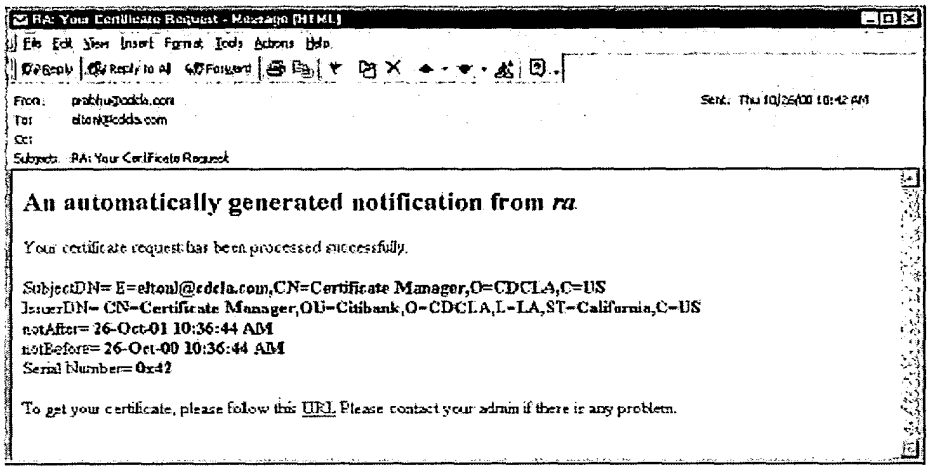


29. The request is then sent to the Certificate Authority (CA). The CA will sign the certificate request and return it to the RA. A copy of the certificate is published in the LDAP database in the 'usercert;binary' field located in the certificate requestor's LDAP user entry.

30. After the CA completes the publishing process, a verification screen will appear, and the RA Administrator can view the details of the issued certificate. When the RA receives the certificate back from the CA, an e-mail is also sent to the certificate requestor indicating that the certificate is ready to be picked up.

31. After the certificate request is approved and a certificate issued by the CA, the e-mail address listed in the certificate enrollment page will get an e-mail similar to the following:

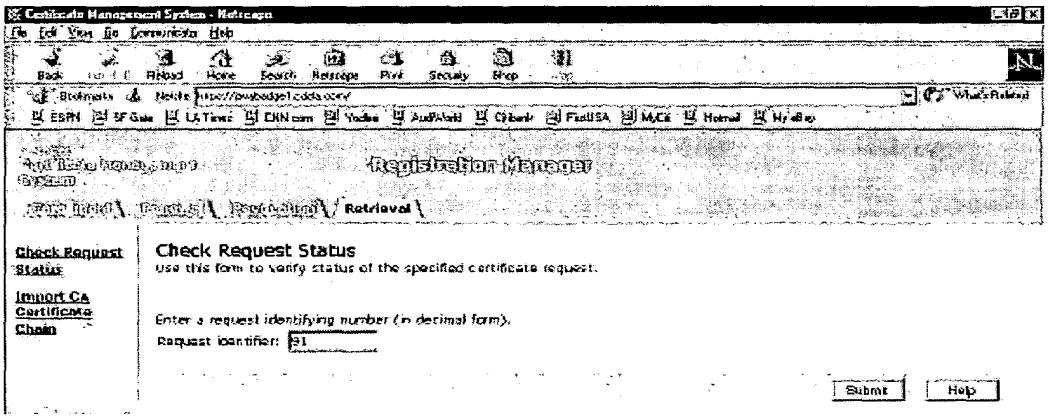
citi



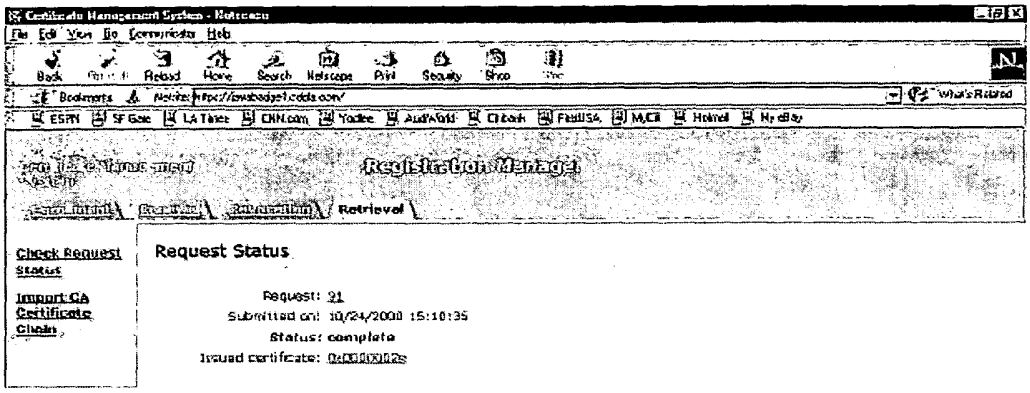
32. At this point, either click on the URL in the e-mail or return to the RA page (https://*hostname.of.RA*).

33. Make sure the new test LCMS Admin Card is inserted in the reader of the PC.

34. When returning to the RA page, the following screen will appear. Click on the 'Retrieval' tab and enter the request identifier that was given when the certificate request was sent. This screen will be bypassed if the user clicked on the URL in the e-mail.



35. If a valid request identifier is entered, the Registration Manager will return a screen with the completed request. NOTE, clicking on the URL in the confirmation email will bring the user directly to this page.



36. Click on the certificate serial number to view the details of the certificate and to verify that it is the correct certificate. Once the information is verified, click on 'Import Certificate'. The certificate will be loaded onto the card automatically.

37. The certificate issuance process is now complete.

38. Attempt authenticating to the test LCMS system with this new card to verify it is active.

39. Mail the test LCMS Admin Card to intended user

citi

40. E-mail card PIN to the intended user